ABSTRACT

Title of dissertation: LOCALLY RECOVERABLE CODES FROM ALGEBRAIC CURVES

Sean Ballentine, Doctor of Philosophy, 2018

Dissertation directed by: Professor Alexander Barg
Department of Electrical & Computer Engineering
Department of Mathematics

Professor Thomas Haines
Department of Mathematics

Locally recoverable (LRC) codes have the property that erased coordinates can be recovered by retrieving a small amount of the information contained in the entire codeword. An LRC code achieves this by making each coordinate a function of a small number of other coordinates. Since some algebraic constructions of LRC codes require that $n \leqslant q$, where n is the length and q is the size of the field, it is natural to ask whether we can generate codes over a small field from a code over an extension. Trace codes achieve this by taking the field trace of every coordinate of a code. In this thesis, we give necessary and sufficient conditions for when the local recoverability property is retained when taking the trace of certain LRC codes.

This thesis also explores a subfamily of LRC codes with hierarchical locality (H-LRC) which have tiers of recoverability. We provide a general construction of codes with 2 levels of hierarchy from maps between algebraic curves and present several families from

quotients of curves by a subgroup of automorphisms. We consider specific examples from rational, elliptic, Kummer, and Artin-Schrier curves and examples of asymptotically good families of H-LRC codes from curves related to the Garcia-Stichtenoth tower.

LOCALLY RECOVERABLE CODES FROM ALGEBRAIC CURVES

by

Sean Ballentine

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2018

Advisory Committee:
Professor Alexander Barg, Co-Chair/Advisor
Professor Thomas Haines, Co-Chair/Advisor
Professor Patrick Brosnan
Professor Lawrence Washington
Professor William Gasarch (Dean's Representative)

Dedication

To my wife Patricia, for her support and patience after all this time.

Acknowledgments

I cannot thank my wife Patricia enough for her support and patience during my time in graduate school. She could not have been more supportive during every long night and early morning these past many years. Even the most stressful of days were made easy because I knew I was coming home to her and our amazing dogs. I am so excited to step into this next stage of my life not only as a recipient of a doctorate in mathematics, but also as her husband.

I would like to thank Dr. Thomas Haines for his insights and direction early on in my time in graduate school. The advice he gave to me during crucial parts of my time at the University of Maryland have shaped my experience in an extremely positive way.

I thank Dr. Alexander Barg for advising me on my thesis problems and providing much needed guidance. I learned a lot from him, not only about the subject of mathematics, but about what it takes to be a working mathematician. His dedication to mathematics, and specifically the coding theory community, was inspiring.

One of the most influential people in my journey in mathematics has been my best friend Alex Youcis. Working with him many years ago completely changed my perspective on mathematics. Without him, I would not be where I am today. Outside of math, he has been an amazing friend and remains someone I admire for his character and talent.

I have been so extremely lucky in graduate school to have the best cohort of graduate students that a person could ask for. I thank Steve, for being a great person to talk to and amazing resource while I developed as an instructor. I would like to thank Rebecca, who is always up to grab a coffee and chat about fiction. I thank Adam, who is great to discuss

a puzzle with or the latest wacky news stories. Ariella is an amazing friend and always willing to hash through my latest concerns. I thank Ryan, for all the cappuccinos we had together and endless talk of board games and Survivor. Each one of you has made my experience in graduate school one I will always cherish.

I must thank the rest of my friends and family who have supported me over the years in different ways. In particular, I thank Rob, Summer, Matt, Rachel, Stephanie and Arkadiy for being great friends to me. I also would like to thank my sister Joie, whose house was always open to me and my wife when we wanted to get away.

Last, and certainly not least, I thank the friendly faces at the Board and Brew in College Park and in particular, Ben and Zach. I will miss having such a great place to do my work. A lot of the energy that went into this thesis was directly fueled by the endless train of caffeinated drinks that they supplied.

Contents

Chapter 0: Introduction

Digital data transmitted over communication channels or recorded in storage devices is naturally subjected to noise that alters or erases parts of the contents. The need to recover data from noise motivates the main problems of mathematical coding theory. We assume that the data is encoded using a finite field alphabet, and parity checks are added to it to enable recovery from distortions of various kind. The main focus of coding theory is on constructions involving linear encoding of the data which accounts for both rich structure and feasibility of practical implementations.

The focus of this thesis is on problems motivated by applications in distributed storage systems wherein large volumes of data are written on multiple storage drives (nodes). The temporary failure of one or several of these nodes is common and renders the information stored there unavailable for its users. Accordingly, the main usage of coding in such systems is related to combating erasures. At the same time, classical code constructions are designed to correct a large number of erasures, and their use in distributed storage systems leads to a large amount of communication between the storage nodes, which is undesirable. This motivates the problem of designing codes that support recovery of one erasure by reading a small portion of the encoding, while also being able to correct many erasures in the case of massive node failure.

Let $\mathbb{F}_q$ be a finite field and consider an n-dimensional linear space $\mathbb{F}_q^n$. Define the Hamming metric on $\mathbb{F}_q^n$ by setting $d(x, y) := |\{i : x_i \neq y_i\}|$. A linear code C of length n and dimension k is defined as an image of an injective linear map $\mathbb{F}_q^k \to \mathbb{F}_q^n$, i.e., a linear k-dimensional subspace of $\mathbb{F}_q^n$. Elements of C are called codewords. The minimum distance of C is the smallest distance between a pair of distinct codewords. Let d be the minimum distance of C. If a number of coordinates of the codeword are erased, it is possible to recover the entire codeword as long as the remaining part of the codeword identifies it uniquely. Since projecting on any $n - (d - 1)$ coordinates is an injective map, the code corrects up to $d - 1$ erasures. One prominent example of this construction is given by the classic family of *Reed-Solomon codes*, which also serve a starting point for a number of constructions in this thesis. The power of this approach is related to the fact that the remaining (non-erased) coordinates enable us to identify the entire codeword; at the same time, correcting just one erasure can conceivably be done more efficiently.

Locally recoverable codes provide a solution to the above problem. In a locally recoverable code, introduced in [13], each coordinate is a function of a small number r other coordinates. This means that when a failure at a single node occurs, the user can recover the missing data without accessing all the remaining nodes of the encoding. Naturally, the additional dependencies among the coordinates of the code entail the reduction of the dimension of such a code relative to the other parameters. In [35], families of optimal locally recoverable codes of length $\leqslant q$ were constructed that are an extension of Reed-Solomon codes. In [6], this was further extended to $n > q$ using codes generated from maps between algebraic curves.

In this thesis we explore a few problems related to the situation described above. In Chapter 1 of this thesis we cover the necessary background material in more detail. This includes a discussion of linear codes and their parameters and an introduction to some of the main constructions that are important to the later chapters, including Reed-Solomon codes and classical algebraic geometry codes. In Chapter 2 we study a problem in the field of locally recoverable codes that are defined over non-prime finite fields. For a given extension of finite fields, trace codes are codes over the base field that are obtained by taking the trace of every codeword of a code in the extended field. If the original code happened to be locally recoverable it is natural to ask if there is a similar recoverability structure on the resultant trace code. In this chapter we present original results on characterizing when the recoverability is preserved when the LRC code is generated using a certain algebraic geometry construction. In Chapter 3 we examine an extension of locally recoverable codes to codes with hierarchical locality. Briefly, hierarchical codes have multiple levels of recoverability in a tiered structure. We present a new construction that is an extension of the locally recoverable construction on curves. We also construct several code families with hierarchical locality on algebraic curves, including families that have asymptotically good parameters. These results were published in [2] and form the contents of the preprint [3].

0.1 Summary of Results

The results of this thesis are broken up into two main parts, Chapter 2 and Chapter 3, both of which answer questions related to locally recoverable codes. Contained here is

a detailed list of original results presented in this thesis. The results of Chapter 3 were previously published in [2, 3].

Chapter 2 This chapter answers questions related to locally recoverable trace codes. Since many algebraic construction of locally recoverable codes have bounds on the length that depend on the size of the field of definition, it is natural to ask how to generate longer codes by using codes originally defined over some field extension. One way to accomplish this is trace codes which uses the entry-wise field trace. In this chapter we present the following original results:

- Given a covering of the projective line, we prove necessary and sufficient conditions for the local recoverability of the corresponding code to be preserved under the trace map. The characterization of when this happens depends on the covering curve to consist of "good fibers". In this chapter we give a systematic method for generating sets of good fibers.

- We construct an example of an algebraic geometry code that is generated from a curve with good fibers. For this example we compute the resulting paramters of the corresponding trace code.

Chapter 3 This chapter is devoted to a generalization of LRC codes to codes with hierarchical locality. These codes attempt to further approve the efficiency in the repair of failed nodes in distributed storage systems. Codes with hierarchical locality have multiple levels of recoverability, small recovering sets to recover simple node failures efficiently and larger recovering sets to efficiently repair small numbers of concurrent failures. In

Chapter 3, we give new constructions of such codes from maps between algebraic curves and prove some related results:

- We present a generalization of a construction of locally recoverable codes from maps between curves to generate codes with hierarchical locality.
- We give a family of examples of q-ary codes with length $n \leqslant q$ and optimal parameters constructed by taking quotients of rational function fields.
- We give an extension of the above example to length $q+1$ that requires an adjusted construction.
- We also construct codes of length close to $q + 2\sqrt{q}$ constructed from quotients of elliptic curves.
- We construct examples from maps between curves extracted from the Garcia-Stichtenoth tower and inspired by the limitations of the codes generated from the this tower, we generate a class of examples from quotients of Kummer curves that have good parameters.
- Finally, the Garcia-Stichtenoth tower gives rise to several asymptotic results that result in asymptotically good codes with hierarchical locality.

Chapter 1: Background

1.1 Introduction to Coding Theory

We begin by introducing some of the basic definitions required to discuss the theory of codes. We focus on the notions that relate directly to the results of this thesis, in particular the ideas necessary to introduce algebraic geometry codes. We touch on the ideas of classical coding for background, and the problems of interest in the algebraic geometry code setting are introduced in Section 1.3. For more background on coding theory and algebraic geometry codes, see [27], [34], and [38]. This chapter does not contain new results, and references are given for the most important of the cited statements.

1.1.1 Basic Definitions

Let $\mathbb{F}_q$ denote a finite field with q elements and $\mathbb{F}_q^n$ denote the n-dimensional vector space over $\mathbb{F}_q$. For a vector $x \in \mathbb{F}_q^n$ we denote by x_i the i^{th} coordinate of the vector x.

Definition 1.1.1 (Linear code)**.** *An $[n.k]$ linear code C over the finite field $\mathbb{F}_q$ is a k-dimensional sub-space of the vector space $\mathbb{F}_q^n$.*

The vectors that appear in a code C are called *codewords* of C. The parameter n in the definition above is referred to as the *length* of the code. The parameter k is referred to as

the *dimension* of the code. This definition is often extended to a more general definition of codes to include subsets of $\mathbb{F}_q^n$ that are not necessarily linear subspaces. In this thesis all codes are assumed to be linear. There are a few reasons why it is common in the literature to restrict to the class of linear codes. The most important reason is that the linear structure allows for efficient algorithms for using the code.

Definition 1.1.2 (Hamming weight/distance)**.** *Given a vector $x \in \mathbb{F}_q^n$ the Hamming weight of x is defined to be*

$$\mathrm{wt}(x) = \#\{i | x_i \neq 0\}.$$

Given two vectors $x, y \in \mathbb{F}_q^n$, we define the Hamming distance between x and y to be

$$d(x, y) = \mathrm{wt}(x - y) = \#\{i | x_i \neq y_i\}.$$

This definition of distance induces a metric on the vector space $\mathbb{F}_q^n$ and is vital to measuring the performance of error-correcting codes.

Definition 1.1.3 (Dual code)**.** *Given an $[n, k, d]$ code C, define $C^\perp$ as follows*

$$C^\perp = \{x \in \mathbb{F}_q^n | x \cdot y = 0 \ \forall y \in C\}.$$

It is clear from the definition that the dual code of an $[n, k]$ code is an $[n, n - k]$ code. In later chapters we make use of the fact that a nonzero vector, x in $C^\perp$ gives a linear relationship among the coordinates of every codeword c in C called a parity check and given by the equation $x \cdot c = 0$.

Definition 1.1.4 (Minimum distance)**.** *The minimum distance of an* $[n, k]$ *code* C *is defined to be*

$$d_{\min}(C) := \min\{d(x, y)|x, y \in C, x \neq y\}$$

and C *is said to be an* $[n, k, d]$ *code.*

For a fixed value of the code length n, the minimum distance and dimension of the code are competing parameters. This means that codes with large dimension necessarily have low minimum distance and vice versa. Naturally, one might ask how large we can make one parameter while the other is fixed. For a fixed code length and dimension, the following theorem gives an upper bound for the minimum distance.

Theorem 1.1.5 (Singleton bound)**.** *Let* C *be an* $[n, k, d]$ *code, then*

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

Proof. Since the minimum distance is d, the mapping from $C \rightarrow \mathbb{F}_q^{n-(d-1)}$ given by removing the last $d - 1$ coordinates from each codeword is injective. This implies

$$k \leqslant n - (d - 1).$$

□

Codes that meet the Singleton bound are referred to as *maximum distance separable* (MDS) codes. MDS codes do not exist for $n \geqslant 2q$ and are only known to exist for $n \leqslant q + 1$. In Section 1.1.3 we present a naturally occurring class of MDS codes that are

central to this thesis.

1.1.2 Error Correction/Detection

In this section, we introduce the classical problems in information theory that inspire the definitions given in the previous section. In this section we present the problems that arise in the classical setting of error correction/detection. However, it is the erasure model given at the end of this section that is the focus of the rest of this thesis. For simplicity, we consider transmissions consisting of only 4 possible messages: $\{A, B, C, D\}$. Note that choosing an $[n.k]$ linear code is equivalent to choosing an embedding $\mathbb{F}_q^k \to \mathbb{F}_q^n$ called the encoding mapping. In the remainder of this section, we consider three choices of the encoding mapping for the alphabet above.

The Naive Approach - The most obvious choice of encoding is given by

$$A \mapsto (00)$$

$$B \mapsto (10)$$

$$C \mapsto (01)$$

$$D \mapsto (11).$$

While this choice is efficient in keeping messages as short as possible we find that it is not resilient to the natural noise that occurs when transmitting message. For example, if we were to transmit the message CAB by encoding it as (010010) and there is noise in the transmission causing one of the bits to flip. At the receiver end of the communication line,

the message reads as (010011) which decodes to CAD. The receiver receives a corrupted message and, equally important, the receiver is unaware that an error has occurred.

Error Detection - One solution to the error detection problem is to add a check digit to the end of the ecoding of each letter. Consider the following choice of encoding for the same alphabet.

$$A \mapsto (000)$$

$$B \mapsto (101)$$

$$C \mapsto (011)$$

$$D \mapsto (110).$$

Now, to transmit the same message as before, CAB, we encode the message as (011000101). If noise in the transmission were to again flip one of the digits such as (011001101), the receiver will now be unable to decode the message since the middle letter (001) is not a valid letter in our alphabet. The receiver can now request a re-transmission in an attempt to receive a valid version of the message. In this example we chose a $[3, 2, 2]$ code to encode our message compared to the $[2, 2, 1]$ code chosen in the naive approach. The important difference between these examples is that the minimum distance in the second one is greater than 1. Using such a code ensures that any two codewords differ in at least two entries. More generally if we choose a code with minimum distance d, the receiver will detect up to $d - 1$ errors in the transmission.

The consequence for adding check digits to obtain error-detecting codes is a drop in trans-

mission rate and overall efficiency. Not only are the codewords longer but if an error is detected the receiver needs to request a re-transmission of the corrupted codewords. It would be more efficient if the receiver could fix locally any errors that occur.

Error Correction - To allow for local error correction we need even greater separation between the vectors in our code. By increasing the minimum distance even more than we did in the previous example, not only can we ensure that errors are detected but we can recover the original message. Continuing with the examples from above, let us choose our encoding mapping in the following way.

$$A \mapsto (000000)$$

$$B \mapsto (111000)$$

$$C \mapsto (000111)$$

$$D \mapsto (111111).$$

The choices above result in a $[6, 2, 3]$ code. Once again we consider the situation in which a message is transmitted through a noisy channel that results in a single error in the message. For example, our previous message CAB (000111000000111000) may become (000111000000111001). The receiver will detect an error in the last character of the transmitted message and additionally predict that the original character was a B since that is the closest vector with respect to the Hamming distance. This model assumes that errors occur with a low probability so the closest vector is the most likely candidate for the orignal message.

In the example above, if two errors were to occur the receiver may not have be able to correctly decode the message using this method. In general, a code with minimum distance d is able to correct $\lfloor \frac{d-1}{2} \rfloor$ errors in the transmission.

The Erasure Model - There is another model of the above problem that is important for this thesis. In the examples of this section, we assume the model in which errors in transmission result in elements of the message being changed. An alternative model instead assumes that message corruption results in erasures of data at the corrupted coordinates. Erasures are errors with a known location. We call a particular choice or erasure locations an erasure pattern and we say that an erasure pattern is correctable if the codeword can be identified by its remaining coordinates. This occurs when the erasure mapping that takes every codeword and erases the coordinates in the chosen pattern is injective. For linear codes this occurs as long as the erasure mapping applied to any non-zero codeword does not result in the zero vector, i.e., if the number of erasures is less than $d - 1$. This implies, a minimum distance d code can correct any $d - 1$ erasures. To illustrate this let us consider the same example from above.

$$A \mapsto (000000)$$

$$B \mapsto (111000)$$

$$C \mapsto (000111)$$

$$D \mapsto (111111).$$

Now if the message CAB (000111000000111000) is transmitted and two erasures occur,

this may result in the receipt of (0001110000001110 - -). It is still clear at this point that the last character is a B but if one additional erasure occurred at the third to last entry then it is no longer clear whether or not the last character is B or D.

1.1.3 Reed-Solomon Codes

In this section, a class of MDS codes called Reed-Solomon codes is introduced. Algebraic geometry codes are a direct generalization of Reed-Solomon codes which makes them central to understanding their construction. The following construction takes advantage of a very important property of linear codes. Since the code is linear, the entry-wise difference of two codewords results in another codeword. This implies that

$$\begin{aligned} d_{min}(C) &= \min\{d(x,y)|x,y \in C\} \\ &= \min\{\mathrm{wt}(x-y)|x,y \in C\} \\ &= \min\{\mathrm{wt}(c)|c \in C\}. \end{aligned}$$

This means that the problem of maximizing the minimum distance of an $[n,k]$ is equivalent to minimizing the number of zeroes that can occur in a non-zero codeword. We achieve this by taking advantage of the fact that low-degree polynomials have a limited number of zeros.

Definition 1.1.6 (Reed-Solomon Code)**.** *Let* $\Omega = \{P_1, \ldots, P_n\}$ *be a set of elements (points) of* $\mathbb{F}_q$ *and choose* k *such that* $1 \leqslant k \leqslant n$*. Let* $V = \mathrm{span}\{x^i|i = 0, \ldots, k-1\}$ *be*

the k-dimensional $\mathbb{F}_q$-linear space of polynomials of degree less than or equal to $k-1$ over $\mathbb{F}_q$. The $[n,k]$ Reed-Solomon code C is defined to be the image of the map

$$\begin{aligned} \mathrm{ev} : V &\to \mathbb{F}_q^n \\ f(x) &\mapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

Proposition 1.1.7. *An $[n,k]$ Reed-Solomon code is MDS and therefore has minimum distance $n-k+1$.*

Proof. To find the minimum distance of a Reed-Solomon code we take advantage of the fact that for linear codes, finding the minimum distance is equivalent to finding the smallest Hamming weight of a non-zero vector in our code (i.e the non-zero vector with as many zeros as possible). Since our codewords are constructed by evaluating a polynomial of degree less than or equal to $k-1$, t here can be at most $k-1$ zeros in any given non-zero codeword. This implies that the weight of a non-zero codeword is at least $n-(k-1) = n-k+1$. □

The MDS property of Reed-Solomon codes make them ideal candidates for error correction but there are some restrictions on the parameters of a Reed-Solomon code. Since we are selecting values from the field $\mathbb{F}_q$ on which to evaluate the vector space of polynomials, we necessarily have $n \leqslant q$. This limitation motivates the introduction of algebraic geometric codes (i.e., codes on algebraic varieties) in the upcoming sections of this thesis. We focus in algebraic geometry codes from algebraic curves and in this setting the idea is that instead of selecting points on the affine line $\mathbb{F}_q$ we select evaluation points on a

general algebraic curve of higher genus, thus allowing for longer codes.

1.1.4 Relative Parameters

In this section, we examine the following question: How do we compare codes of different lengths to one another? In Section 1.1.1 we introduced two parameter important to the performance of a code, the dimension and minimum distance. If we wish to compare codes of different length we can normalize these parameters relative to the length of the code. This results in the following definition.

Definition 1.1.8 (Relative parameters)**.** *The relative minimum distance is*

$$\delta(C) := d_{\min}(C)/n$$

and the transmission rate $R(C)$ is

$$R(C) := k/n.$$

As before, these are naturally competing parameters so it is natural to ask, for a fixed value of $\delta(C)$, how large can we make the transmission rate $R(C)$? Equivalently for a fixed transmission rate how large can we make the relative minimum distance?

We can generalize this by looking at sequences of codes $C_i \subseteq \mathbb{F}_q^{n_i}$ of increasing length n_i such that $\lim_{i\to\infty} R(C_i) = R$ and $\lim_{i\to\infty} \delta(C_i) = \delta$ both exist. We denote by U the subset of all pairs (R, δ) that arise this way.

Theorem 1.1.9 ([28], [1]). *There exists a continuous function $R = \alpha(\delta)$ on the interval $[0, 1]$ such that*

$$U = \{(R, \delta) | 0 \leqslant R \leqslant \alpha(\delta)\}.$$

The above problem of maximizing a given parameter is equivalent to determining this curve $\alpha(\delta)$. While there are a few theoretical upper bounds for this curve, we focus on lower bounds. Finding a lower bound entails finding families of codes with asymptotic parameters that are as large as possible. The following argument uses a naive 'sphere packing' approach to generate a lower bound for the curve. Surprisingly, this bound remained the best known asymptotic bound for many years.

The Gilbert-Varshamov Bound is based on asymptotic estimates of the volume of balls of a specified radius. We include this result since it is often considered a benchmark for asymptotic results of coding theory. Let $\mathrm{Vol}_q(n, d)$ denote the number of points within a ball of Hamming distance d in $\mathbb{F}_q^n$. Fix $p \in [0, 1-1/q]$ and let $d = np$ (here n is increasing and p remains fixed).

Proposition 1.1.10 ([38], p. 56). *Define the q-ary entropy function as follows:*

$$h_q(x) = x \log_q(q-1) - x \log_q x - (1-x) \log_q(1-x).$$

Then

$$\lim_{n \to \infty} \frac{\log_q \mathrm{Vol}_q(n, d)}{n h_q(\rho)} = 1.$$

Thus, for $d \leqslant n(q-1)/q$ we have $\mathrm{Vol}_q(n, d) \approx q^{n h_q(d/n)}$. Given a choice of $m = q^k$

codewords in our code, we can add another codeword not contained in any of the balls of radius d around the previously chosen codewords as long as $mq^{nh_q(d/n)} \leqslant q^n$. More precisely, we need $k + nh_q(d/n) \leqslant n$. A bound is then attained when $k + nh_q(d/n) = n$. Dividing through by n gives us

$$R + h_q(\delta) = 1.$$

The previous few statements show that the graph of $1 - h_q(\delta)$ lies entirely in U. In other words, $\alpha(\delta)$ is bounded below by the function $1 - h_q(\delta)$. This bound held for a very long time and was believed to be the best possible bound until Goppa introduced algebraic geometry codes [14] which led to an improvement of this bound for $q \geqslant 49$ ([38]). In the upcoming sections, we introduce algebraic geometry codes and show the aforementioned improvement upon the Gilbert-Varshamov bound.

1.2 Algebraic Geometry Codes

In this section we examine a construction of codes from algebraic curves that is a generalization of the Reed Solomon codes generated in Section 1.1.3. All curves considered in this section are projective, smooth, and absolutely irreducible over a fixed finite field $\mathbb{F}_q$.

1.2.1 The $\mathcal{L}$-Construction

Let X be a curve as described above and let $\Omega \subseteq X(\mathbb{F}_q)$ with $|\Omega| = n$, where $X(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$ rational points on X. Choose a positive divisor D such that $\mathrm{Supp}(D) \bigcap \Omega = \varnothing$.

Definition 1.2.1. *Consider the map*

$$\Delta : L(D) \to \mathbb{F}_q^n$$

$$f \mapsto (f(P_1), f(P_2), \cdots, f(P_n))$$

where $\Omega = \{P_1, \ldots, P_n\}$. *We define* $C_{\mathcal{L}}(X, P, D) := \text{image}(\Delta)$.

The resulting code is an $[n, k]$ code where $k = \dim(L(D))$. To get a better idea of the relationship between $n, k,$ and d we mention the following well-known results.

Theorem 1.2.2. *(Riemann-Roch Theorem)*

Let X *be a curve over the field* $\mathbb{F}_q$ *and* D *be a divisor on* X. *Then,* $\dim L(D) \geqslant \deg D + 1 - g$ *where* g *is the genus of* X. *Moreover, if* $\deg D > 2g - 2$, *then* $\dim L(D) = \deg D + 1 - g$.

Proposition 1.2.3. *Let* X *be a curve over the field* $\mathbb{F}_q$ *and* D *be a divisor on* X. *Given* $f \in L(D)$, f *has at most* $\deg D$ *zeros on* X.

Proof. Suppose that f in fact had $t = \deg D + 1$ zeros on X at the points $P_1, \ldots, P_t$. Then f would be a non-trivial function in $L(D - P_1 - \cdots - P_t)$. However, the dimension of $L(D - P_1 - \cdots - P_t)$ must be zero since $\deg(D - P_1 - \cdots - P_t) < 0$. Therefore, f can have at most $\deg D$ zeros on X. □

Proposition 1.2.3 says that the minimum distance of the resulting code $C(X, \Omega, D)_L$ satisfies $d \geqslant n - \deg D$. The Riemann-Roch Theorem implies that

$$k - 1 + g \geqslant n - d$$

or in terms of relative parameters,

$$R - \frac{1}{n} + \frac{g}{n} \geqslant 1 - \delta. \tag{1.1}$$

The above construction is generally used with the choices Ω equal to all affine points on the curve X and D equal to some multiple of the point above infinity.

Reed-Solomon Codes Revisited - As mentioned before, the construction presented above is a direct generalization of Reed-Solomon codes. We can construct Reed-Solomon codes from the choices $X = \mathbb{P}^1$ and $D = (k-1)\infty$.

1.2.2 The AG Bound

In this section we revisit the idea of asymptotic families of codes. The problem of coming up with asymptotically good families of codes, and therefore better bounds for $\alpha(\delta)$, initially put algebraic geometry codes on the map. To understand the connection we first present the following proposition.

Proposition 1.2.4. *Let X_i be a sequence of curves over $\mathbb{F}_q$ such that g_i, the genus of X_i, and n_i, the number of affine points on X_i, both go to infinity and g_i/n_i converges to some value α, then $R + \delta = 1 - \alpha$ is entirely in U.*

Proof. This follows immediately from (1.1) and taking the limit as n goes to infinity. □

Example: Modular Curves.([39]) Let $l \neq p$ be a rational prime and let $\Gamma_0(l)$ be the standard congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$\Gamma_0(l) = \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, c \equiv 0 \bmod l \right).$$

We define the modular curve $X_0(l)$ as the upper-half plane modulo the action of $\Gamma_0(l)$, i.e.

$$X_0(l) = H/\Gamma_0(l).$$

Next, we state a result in the field of modular curves that will be useful for calculating the asymptotic parameters of the codes generated from these curves modulo $\mathbb{F}_{p^2}$.

Lemma 1.2.5. *Asymptotically, as $l \to \infty$, $X_0(l)/\mathbb{F}_{p^2}$ satisfies*

$$N(X_0(l)/\mathbb{F}_{p^2}) \approx g(p-1),$$

where g is the genus of $X_0(l)/\mathbb{F}_{p^2}$ and $N(X)$ is the number of affine points on X.

If we take this sequence of curves $X_0(l)/\mathbb{F}_{p^2}$ as $l \to \infty$ and apply proposition 1.2.4, we get that the curve $R + \delta = 1 - 1/(p-1)$ is in U. This improves upon the Gilbert-Varshamov bound for certain values of the transmission rate R.

1.3 Locally Recoverable Codes

Locally recoverable (LRC) codes form a family of codes motivated by applications in distributed storage that support repair of a failed coordinate by contacting a small number of other coordinates in the code. This is achieved by making each coordinate a function of the values at few other coordinate. The general idea is that using the entire codeword for

a single erasure, which are very common in storage systems, is not efficient enough. We formalize this idea in the following sections and provide some examples of constructions of such codes.

1.3.1 Definitions

Definition 1.3.1 (LRC codes, [13]). *A code $C \subset \mathbb{F}_q^n$ is* locally recoverable with locality r *if for every $i \in \{1, 2, \ldots, n\}$ there exists an r-element subset $I_i \subset \{1, 2, \ldots, n\} \backslash \{i\}$ and a function $\phi_i : \mathbb{F}_q^r \to \mathbb{F}_q$ such that for every codeword $x \in C$ we have*

$$x_i = \phi_i(x_{j_1}, \ldots, x_{j_r}), \tag{1.2}$$

where $j_1 < j_2 < \cdots < j_r$ are the elements of I_i.

For a given coordinate $i \in \{1, \ldots, n\}$ the set I_i is called the *recovering set* of i. We denote by $C|_{\{i\} \cup I_i}$ the restriction of the code C to the coordinates in $\{i\} \cup I_i$ by C_i, and we call the set $\{i\} \cup I_i$ a *repair group*. Note that the length of C_i is $r + 1$.

In this thesis we study only linear LRC codes. For them the above definition can be phrased as follows: For every $i \in \{1, 2, \ldots, n\}$ there exists a punctured code $C_i := C|_{\{i\} \cup I_i}$ such that $\dim(C_i) \leqslant r$ and distance $d(C_i) \geqslant 2$. Since C_i corrects one erasure, every coordinate in the repair group $\{i\} \cup I_i$ can be locally recovered.

In this form, the definition of LRC codes is easily extended to local correction of more than one erasure. Following [20], we say that a linear code has locality (r, ρ) if for every $i \in \{1, 2, \ldots, n\}$ there exists a subset $I_i \subset \{1, \ldots, n\} \backslash \{i\}$ such that the code $C_i = C|_{i \cup I_i}$ has dimension $\dim(C_i) \leqslant r$ and distance $d(C_i) \geqslant \rho$. In this case any $\rho - 1$ erasures can

be locally corrected, and we again refer to the set $\{i\} \cup I$ as a repair group. Although this is not needed in this definition, earlier works assumed that $|I_i| = r + \rho$, and that $\dim(C_i) = r, d(C_i) = \rho + 1$, i.e., that the code C_i is maximum distance separable (MDS); see for instance [6, 35].

Theorem 1.3.2. [13] *Let C be an $[n, k, d]$ code with locality r. The minimum distance of C is bounded above as follows:*

$$d \leqslant n - k + 2 - \lceil k/r \rceil. \tag{1.3}$$

For the correction of $\rho - 1$ erasures locally this bound becomes [20]:

$$d \leqslant n - k + 1 - \left(\left\lceil \frac{k}{r} \right\rceil - 1 \right)(\rho - 1). \tag{1.4}$$

We say that C is an optimal locally recoverable code if its parameters meet the bound (1.3)-(1.4) with equality.

1.3.2 Tamo-Barg Codes

In this section we give a construction of optimal LRC codes first introduced in [35]. They are a direct generalization of the MDS Reed-Solomon codes presented in Section 1.1.3. The codes in [35] are, like Reed-Solomon codes, constructed as evaluations of functions from a k-dimensional linear space $V \subset \mathbb{F}_q[x]$.

Definition 1.3.3. *Let $\Omega = \{P_1, \ldots, P_n\}$ be a collection of $n = (r + 1)m$ values in $\mathbb{F}_q$ equipped with a partition into subsets of size $r + 1$. Let k be such that $r|k$ and let V be*

the k-dimensional subspace of $\mathbb{F}_q[x]$ given by

$$\text{span}\{\phi^j x^i, j = 0, 1, \ldots, k/r - 1, i = 0, 1, \ldots, r - 1\},$$

where $\phi \in \mathbb{F}_q[x]$ is a polynomial of degree $r + 1$ that is constant on each of the partitions of Ω. Then, the Reed-Solomon code is the image of

$$\text{ev} : V \to \mathbb{F}_q^n.$$

The Reed-Solomon codes constructed above are optimal in the sense that they meet the bound (1.3). Indeed, the maximum degree of a polynomial in V is $(\frac{k}{r}-1)(r+1)+(r-1) = k\frac{r+1}{r} - 2$, and therefore, $d_{\min}(C) \geqslant n - k\frac{r+1}{r} + 2$. Moreover, increasing the degree of ϕ from $r + 1$ to $r + \rho - 1, \rho \geqslant 2$ and using the same construction as above with repair groups of size $r + \rho - 1$, we obtain a class of LRC codes whose repair groups can repair up to $\rho - 1$ erasures. For a chosen value of $\rho \geqslant 2$ and for $(r + \rho - 1)|n$ the parameters of these codes meet the bound in (1.4) with equality.

1.3.3 LRC Codes on Curves

The following construction of LRC codes from covering maps of algebraic curves was introduced in [6] and is based on the approach in [35]. Let $\phi : X \to Y$ be a rational separable map of smooth projective absolutely irreducible curves of degree $r + 1$ over a finite field $\mathbb{k}$ and let $\phi^* : \mathbb{k}(Y) \to \mathbb{k}(X)$ be the corresponding map on function fields. Since ϕ is separable, the primitive element theorem implies that there exists a function

$x \in \Bbbk(X)$ such that $\Bbbk(X) = \Bbbk(Y)(x)$. Let $\Omega = \{P_1, \ldots, P_s\}$ be a set of K-rational points on Y and let D be a positive divisor whose support is disjoint from Ω (typically we choose $\text{supp}(D) \subset \pi^{-1}(\infty)$ for a projection $\pi : Y \to \mathbb{P}^1_K$). For each i, let $\{P_{ij}\}$ be the collection of points on X in the preimage of P_i, i.e. $\{P_{ij}\} = \phi^{-1}(P_i)$. We assume that each P_i splits completely in the function field $\Bbbk(X)$, and therefore $|\phi^{-1}(P_i)| = r + 1$ for some fixed integer r and all $i = 1, \ldots, s$. Finally, define the set of points

$$D = \bigcup_{i=1}^{s} \{P_{ij}, j = 1, \ldots, r+1\} \subset X(\Bbbk)$$

that will serve the evaluation points of the code that we are constructing.

Let $\{f_1, \ldots, f_m\}$ be a basis of the linear space $L(Q_\infty)$. These functions can be thought of as functions in $\Bbbk(X)$ by the embedding of function fields ϕ^*, and each of these functions is constant on the fibers of ϕ. Let V be the subspace of $\Bbbk(X)$ of dimension rm spanned over $\Bbbk$ by the functions

$$\{f_j x^i, i = 0, \ldots, r-1, j = 1, \ldots, m\}. \tag{1.5}$$

The code $C(D, \phi)$ is defined as the image of the map

$$\begin{aligned} \text{ev}_D : & V \to \Bbbk^{(r+1)s} \\ & f \mapsto (f(P_{ij}), i = 1, \ldots, s, j = 1, \ldots, r+1). \end{aligned} \tag{1.6}$$

The code $C(D, \phi)$ is locally recoverable with recovering sets of size r. Denote by c_{ij} the coordinate in the codeword that corresponds to the point P_{ij}. The recovering set for c_{ij}

is formed by the r positions given by the points $\{P_{il}, l \neq j\}$ and proceeds by polynomial interpolation. Properties of the codes generated by this construction are well-studied and for more information about their parameters and basic examples of such codes we once again refer the reader to [6].

Chapter 2: Locally Recoverable Trace Codes

2.1 Introduction

Let $\mathcal{C} \subseteq (\mathbb{F}_{q^m})^n$ be a linear code. Recall from Section 1.3 that $\mathcal{C}$ is locally recoverable with recovering set size r if for each index $i = 1, \ldots, n$, the entry at the ith coordinate of any codeword can be recovered from the values at r other coordinates, independent of the codeword. One method for constructing locally recoverable codes, demonstrated in Section 1.3.3, uses techniques of algebraic geometry: we construct the vector subspace $\mathcal{C}$ by evaluating a particular subspace of the function field of a projective curve at certain $\mathbb{F}_{q^m}$-points of the curve. For this construction it is convenient to have many points of the curve defined, meaning that we are tempted to use a larger field of definition. It is then natural to ask how we can obtain codes defined over smaller fields from these codes; for example, it is desirable for applications in computer science to be able to produce codes defined over $\mathbb{F}_2$ from codes defined over larger fields of characteristic 2. In this chapter we examine one method for doing so, namely by taking the image of $\mathcal{C}$ under the trace map $\mathrm{tr} : (\mathbb{F}_{q^m})^n \to (\mathbb{F}_q)^n$, and we seek to answer the natural question of whether the local recoverability of $\mathcal{C}$ is preserved under this map. We determine a specific, easily verifiable

condition on the $\mathbb{F}_{q^m}$-points contained in each recovering set that determines whether the recoverability is preserved in the trace code, and we present examples of curves for which the trace code is locally recoverable.

The Recovering Process

With the setup established in Section 1.3.3, let $v \in V$ be a function on X. Collecting terms with like powers in x, we can write $v = \sum_i (\sum_j a_{ij} f_j) x^i$. Without loss of generality, let us fix the coordinate of the erasure at position $P_{1,r+1}$. On the fiber containing this point, the f_j's are constant (since they are in the image of $K(Y) \hookrightarrow K(X)$), so restricted to this fiber v becomes $v' = \sum c_i x^i$ for some constants $c_i \in K$. To recover the missing coordinate of the codeword we only need to determine the value of the c_i's and then evaluate the polynomial at the missing coordinate. Since by the construction of V the degree of v as a polynomial in x is at most $r-1$, finding the coefficients is possible through polynomial interpolation and therefore we can always recover the missing coordinate.

Let us view this process through a slightly different lens. Finding the missing coordinate through polynomial interpolation is equivalent to finding the unique value b_{r+1} for which the augmented matrix below has a solution:

$$\left(\begin{array}{ccccc|c} 1 & x(P_{1,1}) & x^2(P_{1,1}) & ... & x^{r-1}(P_{1,1}) & b_1 := v(P_{1,1}) \\ . & & & & & . \\ . & & ... & & & . \\ . & & & & & . \\ 1 & x(P_{1,r}) & x^2(P_{1,r}) & ... & x^{r-1}(P_{1,r}) & b_r := v(P_{1,r}) \\ 1 & x(P_{1,r+1}) & x^2(P_{1,r+1}) & ... & x^{r-1}(P_{1,r+1}) & b_{r+1} := v(P_{1,r+1}) \end{array}\right)$$

This system is overdetermined, so there is some linear combination of rows that eliminates the last row of the system and that linear combination is independent of the c_i's. This means that, independent of the choice of function that gives us the codeword, the entries of the codeword along a particular recovering set satisfy some linear relationship. Once this relationship is known for a particular recovering set, the recovering process is simply to use the relationship to evaluate the missing coordinate.

2.2 Trace Codes

There are two natural ways of changing the field of definition of a code, both of which have been studied thoroughly: subfield subcodes and trace codes. The former is a rather naive approach in which we throw away all codewords which have any coordinates that are not already in the basefield. The latter, the construction that we will study, involves applying the standard field trace map to every coordinate of every codeword and looking

at the image of this process. We do not discuss in detail the effects of such processes on the parameters of the code and refer the reader to Chapter 9 of [34] for more details. For now, we review the basic notion of the field trace map.

For an extension of finite fields $\mathbb{F}_{q^m}/\mathbb{F}_q$ the trace of an element $\alpha \in \mathbb{F}_{q^m}$ with respect to this extension is defined as

$$\text{Tr}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}.$$

We can also define the trace of a vector in $\mathbb{F}_{q^m}^n$ as

$$\text{Tr}((\alpha_1, \ldots, \alpha_n)) = (\text{Tr}(\alpha_1), \ldots, \text{Tr}(\alpha_n)).$$

Given a code $\mathcal{C}$ the trace code $\text{Tr}(\mathcal{C})$ is defined as $\{\text{Tr}(C)|C \in \mathcal{C}\}$. Since Tr is an $\mathbb{F}_q$-linear map, it is easy to see that $\text{Tr}(\mathcal{C}) \subseteq (\mathbb{F}_q)^n$ is a vector subspace.

Let's examine briefly what happens when the trace is applied to the codes generated in the previous section. On a particular recovering set, the entries in the codeword prior to the trace being applied satisfy some linear relationship. However, it would be prudent to acknowledge that this is a $\mathbb{F}_{q^n}$-linear relationship that is satisfied. The trace map is not multiplicative and therefore there is no obvious or straightforward approach to how one would find a similar relationship among the entries of the resultant trace codeword.

2.3 Recoverability of the Trace Code

Good fibers

Having described the mechanism by which local recoverablity operates in algebraic geometry codes, and having defined the trace code, we are now ready to embark upon the primary quest of this chapter. As discussed in the introduction, we wish to answer, as completely as possible, the following main question:

Question: Given an LRC code $\mathcal{C} \subseteq (\mathbb{F}_{q^m})^n$ arising from a map $g : X \to Y$ of projective curves as described above, is the trace code $\mathrm{Tr}(\mathcal{C})$ over $\mathbb{F}_q$ also locally recoverable?

For concreteness, we focus here on the case that $g : X \to \mathbb{P}^1_{\mathbb{F}_{q^m}}$ is a projection map. Specifically, we fix the following notation: X is a smooth, projective, absolutely irreducible curve over $\mathbb{F}_{q^m}$, and we fix an affine chart, so that we may identify an open subset $U \subset X$ with the affine variety $\mathrm{Spec}\, \mathbb{F}_{q^m}[x, y]/(f) \subset \mathbb{A}^2_{\mathbb{F}_{q^m}}$, where f is an irreducible polynomial. Restricted to U, g is simply the restriction of the projection map $\mathrm{pr}_2 : \mathbb{A}^2 \to \mathbb{A}^1$. Denote this restriction by $\tilde{g} : U \to \mathbb{A}^1$. We pick distinct elements $y_1, \ldots, y_s \in \mathbb{F}_{q^m}$ such that $\tilde{g}^{-1}(y_i) = \{(x_{ij}, y_i)\}$ for $j = 1, \ldots, r+1$ (in other words, all of the fibers are of size $r+1$ for fixed r). The condition we impose in order to guarantee recoverability of the trace code is a condition on the sets $\{x_{ij}\}$ for each j.

Before describing that condition, let us be precise about how our code is constructed in this particular setup. The function field $\mathbb{F}_{q^m}(X)$ is the field of fractions of $\mathbb{F}_{q^m}[x, y]/(f)$,

which we wish to think of as an extension of the function field $\mathbb{F}_{q^m}(y)$ of $\mathbb{A}^1$ by adjoining the primitive element x satisfying minimal polynomial $f \in \mathbb{F}_{q^m}(y)[x]$. Let $\iota : \mathbb{A}^1 \to \mathbb{P}^1$ take $y \mapsto [1 : y]$, so that restricted to U we have $g = \iota \circ \tilde{g}$, and set $Q_\infty = [0 : 1] \in \mathbb{P}^1$. Pick a positive integer t and set $D = tQ_\infty$. Then we have

$$L(D) = \mathrm{Span}_{\mathbb{F}_{q^m}}\{1, y, \ldots, y^t\}.$$

The vector space of functions that we use to define our code, then, is given by

$$V = \mathrm{Span}_{\mathbb{F}_{q^m}}\{x^i y^j \mid 0 \leqslant i \leqslant r-1,\ 0 \leqslant j \leqslant t\} \subset \mathbb{F}_{q^m}(y)[x]/(f) = \mathbb{F}_{q^m}(X).$$

Letting $P_{ij} = (x_{ij}, y_i) \in U$ for $i = 1, \ldots, s$, $j = 1, \ldots, r+1$, we get our code $\mathcal{C}(D, g)$ as the image of the evaulation map

$$\Delta : V \to (\mathbb{F}_{q^m})^{s(r+1)}$$

given by evaluating a function $F \in V$ at each point P_{ij}.

Let $S = \{y_i\}$ denote the set of y-values that we have chosen. For a fixed index i, write S_i for the set $\{x_{ij} \in \mathbb{F}_{q^m} \mid (x_{ij}, y_i) \in \tilde{g}^{-1}(y_i)\}$. It is on these sets of x-values that we now focus. The following definition describes the property that we will impose on these sets S_i in order to ensure recoverability of the trace code.

Definition 2.3.1. *Let $\mathcal{S} = \{a_1, \ldots, a_k\} \subseteq \mathbb{F}_{q^m}$. We call $\mathcal{S}$ a good fiber over $\mathbb{F}_q$ if there*

exist coefficients $c_1, \cdots, c_k \in \mathbb{F}_q^\times$ *such that*

$$\sum_{i=1}^{k} c_i a_i^j = 0 \text{ for all } 0 \leqslant j \leqslant k-2.$$

Intuitively, this definition arises out of the fact that recoverability on a given fiber comes down to row reducing a matrix of powers of the elements of the fiber over $\mathbb{F}_{q^m}$; if we are in fact able to perform that row reduction over the base field $\mathbb{F}_q$, then the recoverability is preserved by the trace map.

In the general setting, in which the base curve is not necessarily the projective line, there is a similar description of the fibers. The only difference in the code construction is that in place of the recovering coordinate in the polynomials on which we interpolate, we place the image of each point under the primitive element.

Definition 2.3.2. *Let* $g : X \to Y$ *be a map of curves over* $\mathbb{F}_q$ *as described above with primitive element* x*. For any* $\mathbb{F}_q$*-rational point* y *on* Y *we call the fiber* $S_i := g^{-1}(y_i)$ *a good fiber if* $x(S_i)$ *is a good fiber in the previous sense.*

It is important to note here that we are abusing notation by writing $x(S_i)$. We do not mean the image of the set S_i in the traditional sense; if the image of multiple elements of S_i match we consider them separate elements of $x(S_i)$.

Theorem 2.3.3. *Let* $\mathcal{C} \subseteq \mathbb{F}_{q^m}$ *be a locally recoverable code of recovering set size* r *arising from the map* $g : X \to Y$ *as described above. Then the trace code* $Tr(\mathcal{C}) \subseteq \mathbb{F}_q$ *is a locally recoverable code with recovering set size* r *if and only if each of the sets* S_i *is a good fiber.*

Proof. One direction of this theorem is immediate since the trace map is $\mathbb{F}_q$ linear and therefore if the linear relationships that are satisfied are defined over $\mathbb{F}_q$, the same linear relationships are satisfied for every trace codeword along the same recovering sets.

The reverse direction is a little more involved. We use the fact that a code fails to be recoverable if and only if there exists two codewords that agree on a recovering set but do not agree on the position that is to be recovered. In our notation above, if we have a set of evaluation points $S_1, ..., S_{r+1}$ and two functions f_1 and f_2 and an index i_0 such that $f_1(S_i) = f_2(S_i)$ for all $i \neq i_0$ and $f_1(S_{i_0}) \neq f_2(S_{i_0})$ then the code fails to be recoverable.

Now let's assume that one of the sets S_i is not a *good fiber*. Without loss in generality let's assume it is the fiber S_1 which consists of the points $P_1, .., P_{r+1}$. Let $c_1, ..., c_{r+1}$ be the coefficients such that $\sum c_i f(S_i) = 0$ for all f in V. Without loss in generality we can assume that we can scale c_2 to be 1, and since this fiber is not a good fiber, we can assume c_1 is not in the basefield. If we let $f_1 = 0$ then the codeword associated to f_1 will be zero along this recovering set in the original codeword and in the resuting trace codeword. Since functions in V restricted to each recovering set include all polynomials up to degree $r-1$, we can extract a function f_2 that is zero on $x(P_3), .., x(P_{r+1})$ and scaled so that $f_2(x(P_2))$ is some non-zero element of $\mathbb{F}_{q^m}$ that is trace zero. The functions f_1 and f_2 are now rigged so that they agree on $P_2, ..P_{r+1}$ and we need to show that they do not agree at P_1. We know that $\sum c_i f_2(x(P_i)) = 0$ but because of how we chose f_2 this means $c_1 f_2(x(P_1)) + f_2(x(P_2)) = 0$ or that $f_2(x(P_1)) = -c_2^{-1} f_2(x(P_2))$. This means that $\text{Tr}(f_2(x(P_1))) = \text{Tr}(-c_1^{-1} f_2(x(P_2)))$. Since we scaled f_2 to make $f_2(x(P_2))$ an arbitrary trace zero element it turns out that the trace code could only be recoverable if $-c_1^{-1}$ fixed

the set of trace zero elements under multiplication.

The last step will be to show that the only elements in $\mathbb{F}_{q^m}$ that fix the trace zero elements are in the base field. Then, we know that $\text{Tr}(f_2(P_1))$ is non-zero and the trace code is not recoverable. To prove this step, we let $W = \{x \in \mathbb{F}_{q^m} | \text{Tr}(x) = 0\}$, which we think of as a $m-1$ dimensional $\mathbb{F}_q$ vector space of $\mathbb{F}_{q^m}$ and consider the non-degenerate bilinear form $(x, y) \to \text{Tr}(xy)$. $W^\perp$ must be 1 dimensional and it is easy to show that $\mathbb{F}_q \subseteq W^\perp$, therefore $W^\perp = \mathbb{F}_q$. In other words the only elements of $\mathbb{F}_{q^m}$ that fix the trace zero elements are in the base field. □

2.4 Constructions and Examples

Generating Good Fibers

In order for this characterization of good fibers to be of practical use, we wish to investigate two related questions: can we create an exhaustive list of all good fibers living inside $\mathbb{F}_{q^m}$, and can we produce curves with desirable geometric properties that have good fibers? The answer to the first of these is that we have not been able to give an algorithm for generating all good fibers, but we have identified methods of producing large classes of them, described below. The answer to the second is that certain classes of curves, for example trace-norm curves are promising places to look for codes with good fibers ([11]); these are discussed further in the next section.

Let $k \leqslant q$ be a positive integer, and let $v \in \mathbb{F}_q^k$ be a vector such that all coordinates v_i of v

are distinct. By an egregious abuse of notation, write v^s for the vector $(v_i^s) \in (\mathbb{F}_q)^k$, and let

$$V = \mathrm{span}_{\mathbb{F}_q}\{v^s | 0 \leqslant s \leqslant k-2\}.$$

The vectors v^s for $s = 0, \ldots, k-2$ are linearly independent, for a linear relation between them would amount to a degree $k-2$ polynomial over $\mathbb{F}_q$ satisfied by all the v_i, which constitute k distinct values. Hence $\dim V = k-1$. Let $W = V^\perp$, the orthogonal complement with respect to the normal dot product.

Proposition 2.4.1. *Let m be a positive integer, v, W be as defined above, and further assume that there exists a vector $w \in W$ such that w has all non-zero entries. Then the set $S = \{\alpha + \beta v_i | \alpha, \beta \in \mathbb{F}_{q^m}, 0 \leqslant i \leqslant k\}$ is a good fiber in $\mathbb{F}_{q^m}$.*

Proof. The proof is straightforward linear algebra. Let $w = (c_i) \in W$ be a vector with all nonzero entries. Let $0 \leqslant s \leqslant k-2$. Consider the sum

$$\sigma_s = \sum_{i=1}^{k} c_i(\alpha + \beta v_i)^s.$$

We need to show this sum is zero. For $s = 0$ this is clear since c is orthogonal to the all-ones vector v^0. Inductively assume $\sigma_j = 0$ for $j < s$. Expanding the polynomials then gives that $\sigma_s = 0$ if and only if

$$\sum_{i=1}^{k} c_i(v_i)^s = 0,$$

which it does since $c \in W$. □

Classes of Curves With Good Fibers

The Hermitian Curve

The Hermitian curve is a natural place to start when it comes to working out examples. The example is worked out fully for the LRC example in [5]. The affine equation for the Hermitian curve over $\mathbb{F}_{q_0^2}$ is given by $x^{q_0} + x = y^{q_0+1}$. If we use the projection map onto the y coordinate then for each fixed y value the fibers of this map are fibers of the trace map from $\mathbb{F}_{q_0^2}$ to $\mathbb{F}_{q_0}$ and these fibers are *good fibers* in the sense above with coefficient vector of all ones. The resulting code is an LRC code over $\mathbb{F}_{q_0^2}$ with locality $r = q_0 - 1$ and length q_0^3

Let q_0 be 3 and D be the sum of all the affine points in F_9 and Q_∞ be the positive divisor consisting of the single point at infinity. We let t vary over the values 1 to 3 to get a general idea of how trace affects the parameters of these Hermitian codes. We calculate the parameters of the Hermitian codes using the GAP algebra system ([9]) and get the following table:

$r = 2$	$\mathcal{C}$, $q = 9$	Tr($\mathcal{C}$), $q = 3$
t=1	[27,2,23]	[27,3,15]
t=2	[27,4,20]	[27,7,12]
t=3	[27,6,17]	[27,11,8]

To get an idea of how the recovery works, let's examine a few particular codewords in the

$t = 2$ case before and after trace is applied. To generate some codewords we need to pick a function that is in our evaluation space, and for this example we use $f(x, y) = xy - y + x$. This codeword starts as follows:

$$(\alpha^6, \alpha^2, 0, 0, 1, 2, ...).$$

The minimal polynomial of the α here is $\alpha^2 - \alpha - 1$ and the first three values were obtained by evaluating f at the fiber over 0 and the next three values by evaluating f at the fiber over α. As expected, these values add to zero on each fiber ($\alpha^6 + \alpha^2 = 0$) since the coefficient vector is the vector of all ones. This means that this recovery process should pass to the trace code as well. The trace of the above codeword yields:

$$(0, 0, 0, 0, 2, 1...).$$

Now the same relationship holds on these fibers; each group of three adds to zero.

This process works because every fiber of the projection map from the Hermitian curve to $\mathbb{P}^1$ is a *good fiber*. The same will be true for the more general family of norm-trace curves whose fibers under the projection map are fibers of linear maps on the underlying fields.

Evaluating the gap the above codes have with the bound 1.3, we see that the trace codes appear to stray further from being optimal than the original codes. However, the literature suggests that this is to be expected. In [8, 15] that the existence of optimal LRC codes of

very long length relative to q are not possible (mirroring the case for traditional coding and possible lengths of MDS codes). This suggests that in certain cases optimal LRC codes over a field extension may necessarily need to become non-optimal after taking the trace.

2.5 Further Questions

One of the biggest hurdles in generating an even greater set of examples is that there is little known about the parameters of trace codes in general. We would like to apply the above results to families of examples from curves that we know consist of good fibers but we would not be able to say much about the minimum distance of the resulting family over the base field. Additionally, there are many more constructions for LRC codes that could potentially lead to good trace codes over the base field. The above results only apply to the classical algebraic geometry construction. There may be a similar description of the repair groups that is needed for the resulting trace codes to be recoverable.

Chapter 3: Codes with Hierarchical Locality

3.1 Introduction

In this chapter we again examine the problem of local recovery and present an original construction and related results that give a natural extension to locally recoverable codes. While it is common for erasures to occur one at a time, occasionally there may be a need to recover the data from several concurrent coordinate failures. Addressing this problem, several papers have constructed families of LRC codes that locally correct multiple erasures [20, 35]. In this chapter we consider the intermediate situation when the code corrects a single erasure by contacting a small number r_2 of helper nodes, while at the same time supporting local recovery of multiple erasures. This gives rise to LRC codes with hierarchy (H-LRC codes), originally defined in [31]. We observe that the hierarchical locality property arises naturally in constructions of algebraic geometric LRC codes, leading to a general construction of such codes from covering maps in towers of algebraic curves.

Paper [31] obtained an upper bound on the distance of H-LRC codes in terms of the dimension and locality parameters. Codes that meet this bound with equality are called

(distance)-optimal. Optimal H-LRC codes with 2-level locality over $\mathbb{F}_q$ of length $n \leqslant q-1$ were constructed in [31], extending the construction of Reed-Solomon subcodes in [35]. Another generalization of the construction in [35] builds upon a geometric view of these codes, and expands it to locally recoverable codes obtained from covering maps of algebraic curves [6]. Using that approach, several follow-up papers constructed a number of families of LRC codes on curves [4, 17, 19, 22, 23]. In this chapter we further extend the basic construction of LRC codes on curves to construct LRC codes with hierarchy. Our main result is a general construction of such codes from covering maps, and we use it to obtain families of H-LRC codes based on quotient curves and other well-known towers of curves, including quotients of elliptic, Kummer, and Artin-Schreier curves. We also construct H-LRC codes of unbounded length from curves related to the Garcia-Stichtenoth tower [10], observing that they yield an asymptotically good family of codes. Finally, we briefly consider H-LRC codes with multiple recovering sets, addressing the so-called availability problem [30, 35] in the hierarchical setting.

A preliminary version of the work in this chapter was presented at the 2018 IEEE International Symposium on Information Theory [2]. The final version of the study of H-LRC codes, presented in [3], expands [2] by including the material in Sections 3.5-3.7.

3.2 Definitions

In the following definition, due to [31], we introduce linear codes with hierarchical locality, which form the main subject of our paper.

Definition 3.2.1 (H-LRC codes [31]). *Let $\rho_2 < \rho_1$ and $r_2 \leqslant r_1$. A linear code C is H-LRC with parameters $((r_1, \rho_1), (r_2, \rho_2))$ if for every $i \in \{1, \ldots, n\}$ there is a punctured code C_i such that*

1. $\dim(C_i) \leqslant r_1$,
2. $d(C_i) \geqslant \rho_1$, *and*
3. C_i *is an* (r_2, ρ_2) *LRC code.*

The intuition behind this definition is that any $\rho_2 - 1$ erasures can be recovered using the local correction procedure of the code C_i (i.e., using recovering sets of size r_2 within the support $\mathrm{supp}(C_i)$), and any larger number of erasures up to $\rho_1 - 1$ can be recovered using the entire set of coordinates of the code C_i. Below we call the codes C_i the *middle codes* and denote their length by ν. Thus, C_i is a $[\nu, r_1, \rho_1]$ LRC code with locality r_2, and in all our constructions $\rho_2 = 2$ which corresponds to local correction of a single erasure (but see Proposition 3.3.3 and the related discussion). In all of our constructions the coordinate set $[n]$ will be partitioned into disjoint groups of size ν, and thus, the codes C_i coincide for all i within each of the groups, and have disjoint supports otherwise. For the purposes of this chapter, we could incorporate this property into the definition of the H-LRC code.

This definition can be extended by induction to any number of levels of hierarchy in an obvious way, and we denote the set of parameters of a τ-level H-LRC code by $(r_i, \rho_i), i = 1, \ldots, \tau$. A bound on the distance of a τ-level H-LRC code that extends (1.4) to all $\tau \geqslant 1$,

takes the following form [31]:

$$d \leqslant n - k + 1 - \Big(\Big\lceil \frac{k}{r_\tau} \Big\rceil - 1\Big)(\rho_\tau - 1) - \sum_{j=1}^{\tau-1} \Big(\Big\lceil \frac{k}{r_j} \Big\rceil - 1\Big)(\rho_j - \rho_{j+1}). \qquad (3.1)$$

An H-LRC code whose parameters meet this bound with equality will be called *optimal* throughout. In this work we extend constructions of optimal LRC codes in the sense of (1.4)-(1.3) to the hierarchical case. There are several constructions of optimal LRC codes in the literature [18, 20, 24, 26, 32, 35, 37]. Among them we single out the construction of [35] which isolates certain subcodes of Reed-Solomon (RS) codes that have the locality property. This code family relies on an algebraic structure of LRC codes that affords an extension to codes on algebraic curves. The theory of algebraic geometric codes with locality, introduced in [6] and further developed in [4, 19, 23] provides a framework for our study here, and we describe it in the next section.

3.3 H-LRC codes on algebraic curves

In this section we present a natural extension of the construction from Section 1.3.3 that gives rise to LRC codes with hierarchy. Let X, Y, and Z be smooth projective absolutely irreducible curves over a finite field $\mathbb{k}$. Consider the following sequence of maps:

$$X \xrightarrow{\phi_2} Y \xrightarrow{\phi_1} Z, \qquad (3.2)$$

where ϕ_1 and ϕ_2 are rational separable maps of degree $s+1$ and r_2+1, respectively, where $s \geqslant 2, r_2 \geqslant 1$. Define $\psi := \phi_1 \circ \phi_2$. Let $\phi_2^* : \Bbbk(Y) \to \Bbbk(X)$ and $\phi_1^* : \Bbbk(Z) \to \Bbbk(Y)$ be the corresponding maps of the function fields. Let $x \in \Bbbk(X)$ and $y \in \Bbbk(Y)$ be primitive elements of their respective algebraic extensions, i.e., suppose that $\Bbbk(X) = \Bbbk(Y)(x)$ and $\Bbbk(Y) = \Bbbk(Z)(y)$. Let $S = \{P_1, \ldots, P_m\}$ be a collection of points on $Z(\Bbbk)$ that split completely on X, i.e., $|\psi^{-1}(P_i)| = (r_2+1)(s+1)$. Let $D = \bigcup_{i=1}^m \psi^{-1}(P_i), n := |D|$, and let Q_∞ be a positive divisor on Z with support disjoint from S. We assume that $\text{supp}((y)_\infty) \cap \phi_2^{-1}(S) = \varnothing$ and $\text{supp}((x)_\infty) \cap \psi^{-1}(S) = \varnothing$, where $(\cdot)_\infty$ is the polar divisor.

As before, let $\{f_1, \cdots, f_t\}$ be a basis for the space $L(Q_\infty)$. Let V be the vector space of functions over $\Bbbk$ spanned by

$$\{f_i y^j x^k | 1 \leqslant i \leqslant t, 0 \leqslant j \leqslant s-1, 0 \leqslant k \leqslant r_2 - 1\}. \tag{3.3}$$

Let $\nu := (s+1)(r_2+1)$ and note that $n = m\nu$. As in (1.6), define the code $C(D, \{\phi_1, \phi_2\})$ as the image of the evaluation map

$$\begin{aligned} \text{ev}_D : & V \to \Bbbk^n \\ & f \mapsto (f(P), P \in D). \end{aligned} \tag{3.4}$$

Recall that [6] assumed that the function x is injective on the fibers $\{P_{ij}, j = 1, \ldots, r+1\}$ (see Sec. 1.3.3), and that this assumption holds in all the examples considered there. In our setting here, x may not be injective on fibers of the map $\psi := \phi_1 \circ \phi_2$. Let $\deg_\psi(x)$

be the maximum multiplicity of values of x when restricted to a fiber of ψ and let $\deg(x)$ and $\deg(y)$ be the degrees of the maps $x : X \to \mathbb{P}^1$ and $y : Y \to \mathbb{P}^1$.

Proposition 3.3.1. *The code $C = C(D, \{\phi_1, \phi_2\})$ is a 2-level H-LRC code of length $n = m\nu$ with parameters $((r_1, \rho_1), (r_2, \rho_2 = 2))$, where the middle codes are of length $\nu = (s+1)(r_2+1)$, dimension $r_1 = r_2 s$, and distance*

$$\rho_1 \geqslant \max(2(r_2+1) - \deg_\psi(x)(r_2-1), 4). \tag{3.5}$$

We also have

$$\dim(C) = tr_2 s \geqslant r_1(\deg(Q_\infty) - g_Z + 1) \tag{3.6}$$

$$d_{\min}(C) \geqslant n - (\deg(Q_\infty)(s+1) + \deg(y)(s-1))(r_2+1) - \deg(x)(r_2-1), \tag{3.7}$$

where g_Z is the genus of Z.

Proof. The set D of n points is naturally partitioned into subsets of size ν, given by the fibers of the covering map ψ and each of them supports a code $C_\alpha, \alpha = 1, \ldots, n/\nu$ of length ν. The support of each of the codes C_α is further partitioned into repair groups of size $r_2 + 1$ each of which is formed of the coordinates contained in a particular fiber of the map ϕ_2. Restricted to such a fiber, the functions $f_1, \ldots, f_t$ and y are constant, and any function in V becomes a polynomial in x of degree $\leqslant r - 1$. Therefore, C restricted to a fiber of ϕ_2 is an r_2-dimensional code with minimum distance ρ_2 determined by the maximum degree of such a polynomial in x, which is $r_2 - 1$. The length of the restricted

code is r_2, so it is a single parity check code with distance $\rho_2 = 2$. Furthermore, this implies that each of the codes C_α (i.e., C restricted to the fibers of ψ) is an LRC code with parameters $(r_2, 2)$.

It remains to determine the parameters of the codes C_α. First note that the functions $f_1, \ldots, f_t$ are constant on these fibers, and therefore, V restricted to each of them becomes an r_1-dimensional space of functions spanned by

$$\{y^j x^k, j = 0, 1, \ldots, s-1; k = 0, 1, \ldots, r_2\}.$$

The minimum distance of C_α is determined by the maximum number of zeros of a non-zero function in V, restricted to a fiber of ψ :

$$\rho_1 \geqslant \nu - (s-1)(r_2+1) - \deg_\psi(x)(r_2-1),$$

which gives the first term in (3.5). To show that $\rho_1 \geqslant 4$, note that the code C_α corrects any three erasures. Indeed, if they are located in different repair groups of size r_2+1, they can be recovered using the LRC properties of C_α. If at least two of them fall in the same repair group, then the function f in (3.4) can be recovered by Lagrange interpolation across the s groups each of which contains at most one erasure.

Finally, the bounds in (3.6)-(3.7) are obtained by the same arguments applied to the code C in its entirety. □

3.3.1 A family of optimal RS-like H-LRC codes

Using the above ideas, we show how the construction of RS-like codes in [35] can be extended to yield optimal two-level H-LRC codes. Let $\mathbb{k} = \mathbb{F}_q$ and let r_2, r_1, and $n \leqslant q$ be such that $r_1 = sr_2$ and $\nu | n$.

To construct the code we start with choosing a subset D of n points in $\mathbb{k}$ and partition it into disjoint subsets D_α of size ν each. Each of the subsets D_α will support an LRC code of dimension r_1 and distance $r_2 + 3$. The repair groups of this LRC code are of size $r_2 + 1$. Assume that there is a polynomial $\phi_2 \in \mathbb{k}[x]$ of degree $r_2 + 1$ such that it is constant on these repair groups. Further, we choose a polynomial $\phi_1 \in \mathbb{k}[x]$ of degree ν that is constant on each of the subsets D_α.

For a positive integer t, let $V \subseteq \mathbb{k}[x]$ be the tr_1-dimensional space spanned by

$$\{\phi_1^k \phi_2^j x^i,\ i = 0, \ldots, r_2 - 1, j = 0, \ldots, s - 1, k = 0, \ldots, t - 1\}. \tag{3.8}$$

Let us construct a code C by evaluating these functions at the points in D as described in (3.4). The function ϕ_1 is constant on each of the sets D_α, and therefore, the functions in V restricted to each of these sets have degree at most $(s - 1)(r_2 + 1) + r_2 - 1$. This implies that the distance of C_α is at least

$$\begin{aligned} d_{\min}(C_\alpha) &\geqslant \nu - (s - 1)(r_2 + 1) - r_2 + 1 \\ &= r_2 + 3, \end{aligned}$$

which meets the bound (1.3) with equality.

The dimension of the code C is $\dim(V) = tr_1$ and the distance is found by counting the maximum degree of a function in V, and is bounded below as

$$d_{\min}(C) \geqslant n - t(r_1 + r_2 + 1 + s) + r_2 + 3$$

meeting the upper bound in (3.1). We conclude with the following proposition.

Proposition 3.3.2. *Let $n \leqslant q, t \geqslant 1$ and let r_1, r_2 be such that $r_1 = sr_2$ for some $s > 1$ and $\nu | n$. The parameters of the code C are $[n, tr_1, d_{\min} = n - t(r_1 + r_2 + 1 + s) + r_2 + 3]$. Furthermore, C is an optimal H-LRC code with two levels of hierarchy and locality parameters $(r_1, r_2+3), (r_2, 2)$. The middle codes C_α are optimal $[\nu, r_1, r_2+3]$ LRC codes.*

The code family in this proposition is originally due to [31], where it was obtained as an extension of [35], with no connection to the geometric interpretation. Making this connection enables us to increase the code length to $n = q + 1$ in the next section.

By increasing the degree of the map ϕ_2 we can increase the distance ρ_2 from 2 to larger values so that each small repair group is resilient to more than one erasure. More specifically, let $\rho_2 \geqslant 2$, and let r_1, r_2 be such that $r_1 = sr_2$ and $((s + 1)(r_2 + \rho_2 - 1))|n$. Let $\phi_1, \phi_2 \in \mathbb{k}[x]$ be polynomials constant on their respective repair groups, and let $\deg(\phi_2) = r_2 + \rho_2 - 1$ and $\deg(\phi_1) = (r_2 + \rho_2 - 1)(s + 1)$. Define the set of functions $V = \text{span}_{\mathbb{k}}(\phi_1^k \phi_2^j x^i)$ where the indices vary as in (3.8). Finally, construct the code C as the set of evaluations of the functions in V on the points in D. The properties of C are summarized in the following proposition which is proved above.

Proposition 3.3.3. *The code C has length n, dimension tr_1 and distance*

$$d_{\min}(C) = n - tr_1 + 1 - (t-1)(r_2 + \rho_2 - 1) - (ts-1)(\rho_2 - 1).$$

It is an optimal H-LRC code with two levels of hierarchy and locality parameters $(r_1, r_2 + 2\rho_2 - 1), (r_2, \rho_2)$. *The middle codes C_α are optimal* $[(s+1)(r_2+\rho_2-1), r_1, r_2+2\rho_2-1]$ *LRC codes.*

It is also possible to increase the degree of the map ϕ_1 thereby increasing the distance of the codes C_α while still keeping the distance $\rho_2 = 2$. Finally, it is possible to increase the degrees of both the maps ϕ_1, ϕ_2, thereby increasing both ρ_1 and ρ_2. As is easily checked, the resulting codes still retain the optimality properties.

3.4 H-LRC codes from automorphisms of curves

While the previous section introduced a general construction of H-LRC codes on algebraic curves, so far we gave only one concrete example that relies on maps between projective lines. To construct a class of examples, we develop the ideas put forward in a series of recent works in [19, 23], constructing towers of curves in the form of (3.2) from automorphism groups of curves. Let G be a subgroup of $\mathrm{Aut}(X)$ with subgroup H such that $|H| = r_2 + 1$ and $|G| = \nu$. Let $\Bbbk(X)^H$ be the set of H-invariant functions in $\Bbbk(X)$ and let $\Bbbk(X)^G$ be the same for G. Consider the following tower of function fields:

$$\Bbbk(X) \xleftarrow{\phi_2^*} \Bbbk(X)^H \xleftarrow{\phi_1^*} \Bbbk(X)^G, \tag{3.9}$$

where ϕ_1^*, ϕ_2^* are the embedding maps of the function fields. Let g_1 and g_2 be primitive elements of the extensions $\Bbbk(X)^H/\Bbbk(X)^G$ and $\Bbbk(X)/\Bbbk(X)^H$, respectively. Choose places $Q = \{Q_1, \ldots, Q_m\}$ of $\Bbbk(X)^G$ that split completely in $\Bbbk(X)$ (i.e., there are $\nu = (s+1)(r_2+1)$ places in $\Bbbk(X)$ above each Q_i), and let Q_∞ be a positive divisor with support disjoint from Q. Let D be the collection of places in $\Bbbk(X)$ above the places in Q.

Since (3.9) is a particular case of (3.2), the general construction in (3.4) applies. Using it, we obtain a code $C(D, \{\phi_1, \phi_2\})$ with parameters $[n, k, d]$ determined by Proposition 3.3.1. Specifically,

$$n = m\nu,\ k = r_2 st,\ \ t := \dim(L(Q_\infty)) \geqslant 1, \tag{3.10}$$

the distance d is bounded in (3.7), and the locality parameters equal $(sr_2, \rho_1), (r_2, 2)$, where ρ_1 is given in (3.5).

In what follows we give some specific examples.

3.4.1 Automorphisms of rational function fields

Let $\Bbbk(X) = \Bbbk(x)$ be a rational function field. Let us assume that r_2 and s are such that there exists a subgroup G of $\mathrm{Aut}(X) = \mathrm{PGL}_2(q)$ of order $(r_2+1)(s+1)$. We apply the construction (3.9) above to get a tower of rational curves

$$X \xrightarrow{\phi_2} Y \xrightarrow{\phi_1} Z. \tag{3.11}$$

By construction, both the degrees of x and y are 1. We obtain an H-LRC code C with parameters $((r_2 s, \rho_1), (r_2, 2))$ where on account of (3.5),

$$\rho_1 \geqslant \nu - (s-1)(r_2+1) - (r_2-1) = r_2 + 3,$$

Note that this is in fact an exact equality because of the upper bound (1.4). Moreover, as is easily checked, the code C as a whole meets the upper bound (3.1) with equality. We obtain:

Proposition 3.4.1. *Let $n \leqslant q$ be a multiple of $(r_2+1)(s+1)$. Using construction* (3.9) *for the subgroups of the automorphism group of the rational function field, we obtain optimal $[n, k, d]$ H-LRC codes with parameters $((sr_2, r_2+3), (r_2, 2))$.*

These codes are in fact from the same family as the codes constructed in Prop. 3.3.2. However, we can extend this construction to optimal H-LRC codes of length $q+1$ relying in part on the ideas in [19]. Assume that $G < \mathrm{PGL}_2(q), |G| = \nu|(q+1)$, then there exists a subset S of $m := (q+1)/\nu$ rational places of $\Bbbk(X)^G$ that split completely in $\Bbbk(X)$. Let $S = (Q_1, \ldots, Q_m) \subset Z(\Bbbk)$ and let $H < G, |H| = r_2 + 1$. Let P_∞ be the infinite place in $\Bbbk(X)$. W.l.o.g. we can assume that $P_\infty | Q_1$. Let $(y)_\infty$ be the polar divisor of y and assume that $\mathrm{supp}((y)_\infty) \cap \phi_2^{-1}(S) = \varnothing$. As above, let the set of evaluation points be $D = \cup_{i=1}^m \psi^{-1}(Q_i)$, and let the fiber above Q_1 be $P_{11} = P_\infty, P_{12}, \ldots, P_{1,\nu}$. The code C is constructed by evaluating the functions in (3.3) at the points in D. Specifically, C is the

image of the following map:

$$f \in V \mapsto ((x^{-r_2+1}f)(P_{11}), f(P_{12}), \ldots, f(P_{m\nu})) \in \mathbb{k}^{q+1}.$$

The idea of constructing codes on curves whose set of evaluation points D includes the support of Q_∞ (by multiplying by an appropriate degree of the uniformizing parameters) has appeared in the literature, e.g., [38, p.194].

Proposition 3.4.2. *The locality parameters of the code C are $(sr_2, r_2+3), (r_2, 2)$, making it into an optimal 2-level q-ary H-LRC code of length $q+1$.*

Proof. We only need to check that the small (size-(r_2+1)) recovering set that contains P_{11} supports local correction. If the erased coordinate is P_{11}, then its value can be found by regular polynomial interpolation. Otherwise, observe that the function f on this set has the form $f(x) = \sum_{k=0}^{r_2-1} a_k x^k$, where a_k's are constants. Observe that $a_{r_2-1} = (x^{-r_2+1}f)(P_{11})$. The remaining $r_2 - 1$ coefficients of f can be found by Lagrange interpolation from the other $r_2 - 1$ evaluations of f in this set. □

For instance, one can take $n = q + 1 = 28$, obtaining an optimal $[28, 6t, d = 37 - 14t]$ H-LRC code over $\mathbb{F}_{3^3}$ with locality parameters $(r_1 = 6, \rho_1 = 9), (r_2 = 6, \rho_2 = 2)$. Nontrivial examples arise when $t = 1, 2$, and we obtain codes with the parameters $[28, 6, 23], [28, 12, 9]$ that meet the bound (3.1).

3.5 H-LRC Codes of Length $n > q + 1$ constructed from elliptic curves

3.5.1 LRC codes from quotients of elliptic curves

Li et al. [23] introduced a construction of optimal LRC codes on elliptic curves obtained from quotients of the elliptic curve by subgroups of automorphisms. We present this construction in this section and extend to H-LRC codes in the next one.

Let E be an elliptic curve over $k = \mathbb{F}_q$ and let G be a subgroup of the automorphism group Aut(E). Note that the automorphism group is the largest for char$(\mathbb{F}_q) = 2, 3$, and therefore examples given in [23] are given for these cases. In the H-LRC case, since two levels of hierarchy are required, most useful examples arise in the characteristic 2 case when the automorphism group is of size 24 [33].

Let us assume that $|G| = r + 1 = 2s$. Denote the coordinate functions of the automorphisms in G by $\sigma_i((x, y)) = (f_i(x, y), g_i(x, y))$. Assume that the set of x-coordinate functions f_i has size s (in the case of odd characteristic this can be achieved by including in G the negation map on y, i.e., the automorphism $\sigma : (x, y) \to (x, -y)$). Let us index the automorphisms $G = \{\sigma_1, \cdots, \sigma_{r+1}\}$ so that to ensure that $f_{i+s}(x, y) = f_i(x, y)$. Finally, let us assume that there is a point $P = (a, b)$ on E such that the points $P_i = \sigma_i(P)$ are distinct, i.e., P is contained in a totally split fiber of the covering map $\phi : E \to E/G$.

Let us define a function

$$z(x, y) = \prod_{i=1}^{s} \frac{1}{f_i(x, y) - a}.$$

First we note that $\sigma_i(z) = z$ for all $1 \leqslant i \leqslant r+1$. This means that z can be thought of as a function in $k(E/G)$. More importantly, this implies that z is constant on fibers of the covering map ϕ. Powers of the function z will take the place of the functions in the Riemann-Roch space $L(D)$ in the general construction of Sec. 3.3. Also note that the divisor of z is

$$(z) = (r+1)\infty - P_1 \cdots - P_{r+1}.$$

Define functions $w_0 = 1$ and $w_i, i = 1, \ldots, r-1$ in $L_i = L(P_1 + \cdots + P_{i+1})$ such that $L_i = \text{span}\{1, w_1, \cdots, w_i\}$ for $1 \leqslant i \leqslant r-1$. Such a choice is always possible by the Riemann-Roch theorem. Define the space of functions used to construct the code as follows:

$$V = \text{span}\{(z^t, w_i z^j) \,|\, i = 1, \ldots, r-1, 0 \leqslant j \leqslant t-1\}.$$

Let $Q = \{Q_1, \ldots, Q_n\}$ be a union of totally split fibers of the covering map ϕ that does include the fiber formed by the points P_i. The LRC code is obtained from the evaluation map

$$\begin{aligned} \text{ev} : & V \to k^n \\ & f \mapsto (f(Q_1), \ldots, f(Q_n)). \end{aligned}$$

As shown in [23], the resulting codes are optimal with respect to (1.3). The recovering sets of the code are coordinates contained in the same fiber of ϕ. Restricted to a fiber of ϕ, a function in V becomes just a linear combination of the r linearly independent functions w_i, enabling one to recover the missing coordinate.

Remark: Even though [23] did not go beyond the genus 1 case, the above construction can be extended to curves of genus 2 with a only few changes to the definition of the w_i's. Namely, take $w_0 = 1$ as before and let w_i to be a nontrivial function in $L_i = L(P_1 + \cdots + P_{i+2})$ such that $L_i = \text{span}\{w_0, \ldots, w_i\}$ The advantage in applying this construction to genus 2 curves is that they can have larger automorphism groups and more rational points, allowing greater flexibility in choices of the parameters. In particular, paper [23] gives examples of the above construction for maximal elliptic curves that result in optimal LRC codes of length close to $q + 2\sqrt{q}$. With genus two curves we can easily construct optimal LRC codes of length n close to $q + 4\sqrt{q}$, which constitute a family of optimal LRC codes of length larger than reported in the literature (apart from the case of $d = 3, 4$ in [25]). At the same time, so far we have not been able to extend this observation to the case of H-LRC codes.

3.5.2 H-LRC Codes from quotients of elliptic curves

Let E, G, $\{P_i\}$, $\{Q_i\}$ and z be as above. Additionally choose a subgroup $H \leqslant G$ of order $r_2 + 1$. Let $\bar{P}_i$ be the point on E/H below P_i. Let $m + 1 := (r + 1)/(r_2 + 1)$ and suppose the P_i are enumerated such that $\bar{P}_1, \ldots, \bar{P}_{m+1}$ are all distinct.

If E/H is of genus 1, we take $w_0 = 1$ and w_i to be a function in $\bar{L}_i = L(\bar{P}_1 + \cdots + \bar{P}_{i+1})$ for $1 \leqslant i \leqslant m - 1$ such that $\bar{L}_i = \text{span}\{1, w_1, \ldots, w_i\}$ as before. Otherwise, if the genus of E/H is 0, we take $w_0 = 1$ and w_i to be a function in $\bar{L}_i = L(\bar{P}_1 + \cdots + \bar{P}_{i+1})$ for $1 \leqslant i \leqslant m - 1$ such that $\bar{L}_i = \text{span}\{1, w_1, \ldots, w_i, w_i'\}$, where w_i' is any additional

linearly independent function in the Riemann-Roch space $\bar{L}_i$. Note that none of the w_i's have poles at $\bar{P}_{m+1}$.

Let $P_{m+1,1}, \ldots, P_{m+1,r_2+1}$ be the points on E above $\bar{P}_{m+1}$. Take $y_0 = 1$ and y_i to be a function in $L_i = L(P_{m+1,1} + \cdots + P_{m+1,i+1})$ such that $L_i = \text{span}\{1, y_1, \ldots, y_i\}$. For clarity, we define the space of functions in two steps. Define V' and V as follows:

$$V' = \text{span}\{w_{m-1}, w_j y_k | 0 \leqslant j \leqslant m-2, 0 \leqslant k \leqslant r_2 - 1\}$$

$$V = \text{span}\{z^t, z^i g | 0 \leqslant i \leqslant t-1, g \in V'\}.$$

Once again the code C is obtained by evaluating the points in Q at all the functions in V. Construct the code C evaluating the functions in V at the points in Q (cf. (3.4)). This results in the following proposition which is proved above.

Proposition 3.5.1. *The code C constructed above is an $[n, k, d]$ H-LRC code with locality parameters $((r_1, \rho_1), (r_2, \rho_2 = 2))$ where*

$$r_1 = r_2(m-1) + 1$$

$$r_2 + 1 \leqslant \rho_1 \leqslant 2r_2 + 2$$

$$k = t(r_2(m-1) + 1) + 1$$

$$d \geqslant n - (t(m+1)(r_2+1) - (r_2+1)).$$

Proof. The middle codes have length $\nu = (m+1)(r_2+1)$ and dimension $r_1 = \dim(V') = r_2(m-1)+1$ since the function z is constant on the fibers of $E \to E/H$. Also, restricted to

a fiber, the functions in V' are contained in $L(\bar{P}_1+\cdots+\bar{P}_m)\cup L(\bar{P}_1+\cdots+\bar{P}_{m-1}+\bar{P}_{m+1})$. This implies that the minimum distance of the middle codes satisfies $\rho_1 \geqslant \nu - m(r_2+1) = r_2+1$. The upper bound on ρ_1 follows from the Singleton bound (1.3).

The value of the dimension k follows directly from the construction. Finally, since $V \subseteq L(t(P_1+\cdots+P_{r+1})-\bar{P}_{m+1}) \cup L(t(P_1+\cdots+P_{r+1})-\bar{P}_m)$ we have

$$d > n - (t(m+1)(r_2+1) - (r_2+1)).$$

□

3.5.3 Examples:

For any even m there exists $\gamma \in \mathbb{F}_{2^m}$ such that the elliptic curve $E : y^2 + y = x^3 + \gamma$ is maximal in the sense that the number of rational points on E meets the Hasse-Weil bound [23, Lemma 3.3]. The automorphism group of E is of order 24, which is also maximal since an elliptic curve can have at most 24 automorphisms. The automorphisms are given by the following coordinate functions:

$$\sigma_x(x,y) = u^2x + s, \quad \sigma_y(x,y) = y + u^2sx + t,$$

where $u^3 = 1, s^4 + s = 0, t^2 + t + s^6 = 0$. The subgroup G of Aut(E) given by restricting s to be 0 or 1 is order 12 and we take H to be the order 4 subgroup of G given by further

restricting u to be 1. By the Riemann-Hurwitz [33, p.37] formula we have

$$2g(E) - 2 \geqslant 2g(E/G) - 2 + \sum_{P \in E(K)} (e_P - 1),$$

where $g(E)$ and $g(E/G)$ are the genus of E and of E/G, respectively, and e_P is the ramification index of the point P. Note that we use the Riemann-Hurwitz formula in the inequality form because in characteristic 2 some of the points are wildly ramified. For instance, let us take $q = 64$. Since the point at infinity is totally ramified, the above equation implies that in the worst case there are 13 additional ramified affine points on E and therefore, there are at least 67 unramified points. Since the order of G is 12, this implies that there are in fact at least 72 unramified points. This results in at least 60 evaluation points on E. The general code construction in this case gives an $[n = 60, k = 4t + 1, d]$ H-LRC code with locality parameters $((4, \rho_1), (3, 2))$ where $4 \leqslant \rho_1 \leqslant 7$ and

$$d \geqslant n - 12t + 4, 1 \leqslant t \leqslant 5.$$

Note that we do not have enough information to determine the distance of the "middle" codes C_1, making it difficult to compare the value of d with the upper bound (3.1). Substituting $\rho_1 = 4$, we obtain

t	k	d
1	5	$52 \leqslant d \leqslant 53$
2	9	$40 \leqslant d \leqslant 46$
3	13	$28 \leqslant d \leqslant 38.$

To obtain examples of length $n > q$, we should take a larger-size field, for instance let us take $\mathbb{F}_{256}$. Applying the same arguments as above, we obtain H-LRC codes with parameters $[264, 4t+1, d]$ and locality $((4, \rho_1), (3, 2))$ where $4 \leqslant \rho_1 \leqslant 7$ and

$$d \geqslant n - 12t + 4, 1 \leqslant t \leqslant 22.$$

3.6 Some families of curves and associated H-LRC codes

While Proposition 3.3.1 gives a general approach to constructing H-LRC codes, estimating the parameters for a given curve is a difficult question, in particular because controlling the multiplicity $\deg_\psi(x)$ in (3.5) is not immediate. The largest distance ρ_1 is obtained if the function x is injective on the fibers of ψ, i.e., if $\deg_\psi(x) = 1$. In this section we present two general constructions that make this possible using properties of the automorphism groups of curves. Thus, all the H-LRC code families constructed below in this section share the property of having distance-optimal middle codes.

3.6.1 Kummer curves

The simplest and at the same time rather broad class of examples arises when $G < \mathrm{Aut}(X)$ is a cyclic group of order not divisible by the characteristic, i.e., when X is a Kummer curve.

Recall that a Kummer curve X over $\mathbb{F}_q$ is defined by the equation

$$y^m = f(x), \tag{3.12}$$

where $m|(q-1)$ and $f(x) \in K := \mathbb{F}_q(x)$ [34, pp.122ff.], [38, p.168]. The field $L := \mathbb{F}_q(x,y)$ is a degree m cyclic extension of K, and any cyclic extension of degree m can be written in this form. The following examples of Kummer curves are maximal and lead to H-LRC codes with good parameters.

1. The *Hermitian curve* $X : y^{q_0+1} = x^{q_0} + x$ over the field $\mathbb{F}_q, q = q_0^2$ is a maximal Kummer curve.

2. The *Giulietti-Korchmáros curves* [12] are given by the affine equation

$$y^{q_0^3+1} = x^{q_0^3} + x - (x^{q_0} + x)^{q_0^2-q_0+1},$$

   and have genus $g = \frac{1}{2}(q_0^3+1)(q_0^2-2)+1$. They are maximal over $\mathbb{F}_q$ for $q = q_0^6$.

3. (The *Moisio curves* [29]) Let $h \in \{0,\ldots,l\}$, let $m|(q_0^l+1)$ and let $q = q_0^n$. Let L be an $\mathbb{F}_{q_0}$-subspace of dimension h in $\mathbb{F}_q$ and suppose that

$$\prod_{\alpha \in L}(x-\alpha) = \sum_{i=0}^{h} a_i x^{q_0^i}.$$

   Let

$$R(x) = \sum_{i=0}^{h} a_i^{q_0^{2n-i}} x^{q_0^{h-i}}.$$

Then the curve given by $y^m = R(x)$ is maximal over $\mathbb{F}_{q^2}$ of genus $(m-1)(q_0^h-1)/2$, so

$$|X(\mathbb{F}_q)| = q_0^{2l} + (m-1)(q_0^{l+h} - q_0^l) + 1.$$

Let $G_0 = \text{Gal}(L/K)$ be the cyclic group of order m. The action of G_0 on the curve X is given by $(x, y) \mapsto (x, \alpha y)$, where $\alpha \in \mathbb{F}_q, \alpha^m = 1$. If m is well-decomposable, say $m = (a+1)(b+1)c$, then one can easily find subgroups $H < G < G_0 \subseteq \text{Aut}(X)$ with desirable properties. Indeed, let m be as above and let α be a generator of G_0. Then we can take $G = \langle \alpha^c \rangle, H = \langle \alpha^{(b+1)c} \rangle, |G| = (a+1)(b+1), |H| = a+1$. It is clear that the invariants of any subgroup of G_0 are generated by powers of y, for instance, from (3.12), y^{a+1} is unmoved by any power of $\alpha^{(b+1)c}$, etc.

Specializing the construction (3.9), we obtain

$$\Bbbk(X) = \Bbbk(x, y) \hookleftarrow \Bbbk(X)^H = \Bbbk(x, y^{a+1}) \hookleftarrow \Bbbk(X)^G = \Bbbk(x, y^{(a+1)(b+1)}).$$

Now it is clear that the primitive element y is injective on the fibers of $\phi : X \to X/G$, and we can use the general code construction with $\deg_\psi(y) = 1$.

Using the general construction of Proposition 3.3.1 for the curves listed above, we obtain several families of H-LRC codes. The case of Hermitian curves is analyzed below in Section 3.7 in the context of power maps (see Example 3.7.3).

Turning to the Giulietti-Korchmáros curves, we observe that the total number of rational points on the curve $|X(\mathbb{F}_q)|$ equals $q_0^8 - q_0^6 + q_0^5 + 1$ (which meets the Hasse-Weil bound

$N(X) \leqslant q + 1 + 2\sqrt{q}g$). Setting aside the point at infinity, we observe that the projection map on x is ramified in at most q_0^3 places, leaving $n \geqslant q_0^8 - q_0^6 + q_0^5 - q_0^3$ totally split places which form the evaluation set D. Now we use Proposition 3.3.1 to claim the existence of H-LRC codes with the following parameters:

$$n \geqslant (q_0^5 - q_0^3)(q_0^3 + 1),\ k = \dim(L(Q_\infty))ab$$

$$d \geqslant n - \deg(Q_\infty)(a+1)(b+1) - q_0^3(ab + b - 2)$$

$$r_2 = a,\ \ \rho_2 = 2$$

$$r_1 = ab,\ \ \rho_1 = a + 3$$

(note that $\deg(y) = q_0^3$). To obtain specific examples, we may take $q_0 = 4$, getting $a = 4, b = 12, c = 1$ or $q_0 = 17$, in which case the decomposition $q_0^3 + 1 = 2 \cdot 27 \cdot 7 \cdot 13$ leaves multiple options for the localities of the codes, etc. We note that the distance of the middle codes is the largest possible, meeting the bound (1.4) with equality.

For the Moisio curves, the size of the ramification set is at most q_0^h, leaving at least $q_0^{2l} + (m-1)(q_0^{l+h} - q_0^l) - q_0^h$ points for the evaluation set D. The codes from the Moisio curves are constructed over $\mathbb{F}_{q^2}$ and have the following parameters:

$$n \geqslant q_0^{2l} + (m-1)(q_0^{l+h} - q_0^l) - q_0^h,\ k = \dim(L(Q_\infty))ab$$

$$d \geqslant n - \deg(Q_\infty)(a+1)(b+1) - q_0^h(ab + b - 2)$$

$$r_2 = a,\ \ \rho_2 = 2$$

$$r_1 = ab,\ \ \rho_1 = a + 3.$$

For instance, we can take $q_0 = 2, l = 5$, and then taking $m = q_0^l + 1$, we obtain H-LRC codes with localities $r_1 = 10, r_2 = 20$, etc.

3.6.2 Artin-Schreier curves

Let $q = q_0^e$ for some $e \in \mathbb{N}$. A curve with the affine equation

$$y^{q_0} - y = f(x) \tag{3.13}$$

for $f(x) = \mathbb{F}_q(x)$ is called an *Artin-Schreier curve* [34, pp.127ff.], [38, p.173]. More generally, a *generalized* Artin-Schreier curve is given by the equation

$$P(y) = f(x), \tag{3.14}$$

where $P(y) = a_u y^{q_0^u} + a_{u-1} y^{q_0^{u-1}} + \cdots + a_0 y, a_0 \neq 0$ is a linearized polynomial whose roots form a linear subspace of $\mathbb{F}_q$. Such a curve X forms a Galois covering of the projective line with the Galois group $G_0 := \text{Gal}(X/\mathbb{P}^1) \cong \mathcal{L}(P)$ where $\mathcal{L}(P)$ is a linear space of roots of $P(y)$ in $\mathbb{F}_{q_0}$ (thus, for coverings of the form (3.13), $G_0 \cong \mathbb{F}_{q_0^u}^+$). The group G_0 acts on the points of X by $(x, y) \mapsto (x, y + \alpha)$ for $\alpha \in G_0$. Artin-Schreier covers give many examples of curves that are either maximal or close to maximal. Examples of maximal curves include the following families.

1. The Hermitian curves given by the equation $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$,

2. The Moisio curves (to see that they are Artin-Schreier, interchange x and y in their

definition).

These examples are maximal in the sense that they attain the Hasse-Weil bound on the number of points.

(3) The Suzuki curves given by

$$S_q : y^q + y = x^{q_0}(x^q + x)$$

where $q_0 = 2^n, q = 2^{2n+1}$ [16]. The genus $g(S_q) = q_0(q-1)$ and the number of $\mathbb{F}_q$-points is $N(S_q) := |X/\mathbb{F}_q| = q^2 + 1$ (i.e., they fill the entire affine plane over $\mathbb{F}_q$). The Suzuki curves are maximal because $N(S_q)$ meets the Oesterlé bound for their genus. The full group Aut(S_q) is the Suzuki group (hence the name), and it contains a subgroup isomorphic to $\mathbb{F}_q^+$ which acts as before by $y \mapsto y + \alpha$.

In each of the cases (1)-(3) above we have

$$\text{Aut}(X) \supseteq G \cong (\mathbb{Z}/p\mathbb{Z})^{e_2} \supset H \cong (\mathbb{Z}/p\mathbb{Z})^{e_1} \tag{3.15}$$

for $q = p^e \geqslant 9$ and some exponents e, e_1, e_2.

Determining the primitive elements of the extensions in (3.9) with the above choice of G and H is generally not an easy question. We limit ourselves to two simple examples.

1. Let

$$X : \ y^q - y = f(x) \tag{3.16}$$

where $q = r^2, r = p^m \geqslant 3$, and let $G \cong (\mathbb{Z}/p\mathbb{Z})^{2m}, H \cong (\mathbb{Z}/p\mathbb{Z})^m$. In this case G acts on $\Bbbk(x, y)$ by fixing $\Bbbk(x)$, i.e., we have $Z = \mathbb{P}^1$ in (3.2) or $\Bbbk(x, y)^G = \Bbbk(x)$ in (3.9). Let H be a copy of $(\mathbb{Z}/p\mathbb{Z})^m$ in $\mathbb{F}_q^+$ with the property that $\alpha^r = -\alpha$ for all $\alpha \in H$. In other words, $G \cong \mathbb{F}_r^+ \oplus \alpha\mathbb{F}_r^+, H \cong \alpha\mathbb{F}_r^+$, where $\alpha^r = -\alpha$. Further, let $z = y^r + y$, then z is invariant under the action $y \mapsto y + \alpha$:

$$(y + \alpha)^r + (y + \alpha) = y^r + y = z.$$

Further,

$$z^r - z = (y^r + y)^r - (y^r + y) = y^q - y = f(x),$$

and thus, $\Bbbk(x, y)^H = \Bbbk(x, z)$, and (3.9) takes the form $\Bbbk(x, y) \supset \Bbbk(x, z) \supset \Bbbk(x)$.

On account of (3.10), we obtain a family of 2-level $[n, k, d]$ H-LRC codes, where $n = m\nu, k = r_2st$, and $\nu = r^2, r_2 = s = r - 1, r_1 = (r - 1)^2, \rho_1 = r + 2, \rho_2 = 2$.

2. Let us again take X in the form (3.16) where this time $q = r^3, r = p^m \geqslant 3$, and let $G \cong (\mathbb{Z}/p\mathbb{Z})^{3m}, H \cong (\mathbb{Z}/p\mathbb{Z})^m$. Let $z = y^r - y$ and note that z is fixed by the action of H on $\Bbbk(x, y)$, and thus $\Bbbk(x, y)^H = k(x, z)$. Further,

$$z^{r^2} + z^r + z = y^q - y = f(x).$$

The tower (3.9) has the form $\Bbbk(x, y) \supset \Bbbk(x, z) \supset \Bbbk(x)$ since G fixes the rational function field in $\Bbbk(x, y)$.

On account of (3.10), we obtain a family of 2-level $[n, k, d]$ H-LRC codes, where

$n = m\nu, k = r_2st$, and $\nu = r^3, r_2 = r-1, s = r^2-1, r_1 = sr_2, \rho_1 = r+1, \rho_2 = 2$.

This example can be further generalized to the curve X of the form (3.16), where $q = r^h, r = p^m$ and $G \cong \mathbb{F}_q^+, H \cong \mathbb{F}_r^+$. The tower (3.9) that gives rise to the code family, has the form $\Bbbk(x,y) \supset \Bbbk(x,z) \supset \Bbbk(x)$, where $z = y^r - y$ and

$$z^{r^h} + z^{r^{h-1}} + \cdots + z = y^q - y = f(x)$$

We obtain a family of 2-level H-LRC codes with the parameters $\nu = r^h, s = r^{h-1} - 1, r_2 = r-1, r_1 = sr_2, \rho_1 = r+2, \rho_2 = 2$.

Remark 3.6.1. *One can consider "mixed" Artin-Schreier–Kummer curves of the form $P(y^m) = f(x)$ over $\mathbb{F}_q$ where m is a linearized polynomial and $m|(q-1)$, and apply arguments similar to the above. However, we are not aware of good examples of such curves although is it likely that they exist.*

Remark 3.6.2. *It is also clear that the above construction can be generalized to more than two levels of hierarchy. Accomplishing this depends on the factorization of $q-1$ for the Kummer case and does not require new algebraic ideas. A similar observation applies to the Artin-Schreier case.*

3.7 H-LRC codes from the Garcia-Stichtenoth tower

In this section we use the general construction of H-LRC codes for curves in the GS tower. We begin by directly applying the idea of Section 3.3 and consider mappings between the

curves two levels apart in the tower, viz. (3.2). This approach meets a complication in that it is not easy to find the multiplicity $\deg_\psi(x)$. We circumvent this difficulty using power maps in Section 3.7.2, which are related to the constructions from Kummer covers in the previous section.

3.7.1 Naive construction

Let $q = q_0^2$ be a square and $\Bbbk = \mathbb{F}_q$. For any $l \geqslant 2$ define the curve X_l inductively as follows:

$$\left.\begin{array}{c} x_0 := 1, X_1 = \mathbb{P}^1, \Bbbk(X_1) = \Bbbk(x_1); \\ X_l : z_l^{q_0} + z_l = x_{l-1}^{q_0+1}, \text{ where for } l \geqslant 3 \\ x_{l-1} := \frac{z_{l-1}}{x_{l-2}}. \end{array}\right\} \tag{3.17}$$

The curves $X_l, l \geqslant 2$ form a tower of asymptotically maximal curves [10].

The authors of [6] constructed LRC codes from covering maps between consecutive curves in this tower. Similarly, we construct H-LRC codes with 2-fold hierarchy by extracting sub-towers of 3 curves from the full tower. Let $\phi_l : X_l \to X_{l-1}$ be the natural projection on the coordinates $x_i, i = 1, \ldots, l-1$. Consider the following subtower of curves with their projection maps:

$$X_{j+2} \xrightarrow{\phi_{j+2}} X_{j+1} \xrightarrow{\phi_{j+1}} X_j. \tag{3.18}$$

Let $x = x_{j+2}$ and $y = x_{j+1}$ be primitive elements such that $\Bbbk(X_{j+2}) = \Bbbk(X_{j+1})(x)$ and $\Bbbk(X_{j+1}) = \Bbbk(X_j)(y)$ (see (3.2)). In this case $\deg(y) = q_0^j$ and $\deg(x) = q_0^{j+1}$ are the

degrees of the maps $X_{j+i} \to \mathbb{P}^1, i = 1, 2$, respectively. Let S be formed of all the affine points of $X_j(\mathbb{k})$ that map to $\mathbb{k}^*$ under the map $\phi_1 \circ \cdots \circ \phi_j$. Let $n_j = q_0^{j-1}(q_0^2 - 1)$ be the size of S, i.e., number of points above $\mathbb{k}^*$ on $X_j, j = 1, 2, \ldots$. Let $Q_{\infty,j}$ to be the point at infinity on X_j and let $t = \dim(L(\ell Q_{\infty,j}))$, where $g_j \leqslant \ell \leqslant n_j$ and g_j is the genus of X_j. Finally, denote $\psi_{j+2} = \phi_{j+1} \circ \phi_{j+2}$.

Using the general construction of Sec. 3.3 for the tower of curves described in (3.18), it is possible to obtain a family of linear H-LRC codes with two levels of hierarchy.

Proposition 3.7.1. *For any $j \geqslant 1$ there exists a family of H-LRC codes with the parameters $[n, k, d]$ and locality $(r_1, \rho_1), (r_2, \rho_2 = 2)$, where*

$$n = q_0^{j+1}(q_0^2 - 1)$$

$$k = t(q_0 - 1)^2 \geqslant (\ell - g_j + 1)(q_0 - 1)^2$$

$$d \geqslant n - \ell q_0^2 - 2q_0^{j+1}(q_0 - 2)$$

and $r_1 = (q_0 - 1)^2, r_2 = q_0 - 1$,

$$\rho_1 \geqslant \max(2q_0 - \deg_{\psi_{j+2}}(x)(q_0 - 2), 4).$$

Proof. Apply the construction of Proposition 3.3.1 to the curves in Eq. (3.18). The length of the obtained code equals the size of the evaluation set D, which is taken to be $|X(\mathbb{F}_q)| - 1 - q_0^{j+1}$, accounting for removing the point at infinity as well as the q_0^{j+1} ramified points above $0 \in \mathbb{P}^1$ on X. All the other parameters are found directly from Proposition 3.3.1.

□

The shortcoming of the above construction is that it is unclear how to choose the primitive element x such that $\deg_{\psi_{j+2}}(x)$ is small enough to guarantee a large value of the minimum distance of the middle code ρ_1. It would be preferable if we could limit $\deg_{\psi_{j+2}}$ to 1 since this would force the middle code to be an optimal LRC code by itself.

3.7.2 H-LRC codes from power maps

To overcome the shortcomings of the previous construction, in this section we present a construction of H-LRC codes from the curves in the GS-tower for which the primitive element x of the map constructed is naturally injective on the fibers of the map $\psi : X \to Z$ where $X = X_j$ is a GS curve and Z is a quotient curve that we are going to construct. Define the curve $X_{j,c}$ by its function field

$$\Bbbk(X_{j,c}) = \Bbbk(x_1^c, x_2, \ldots, x_j),$$

where the variables x_i are defined as above in (3.17). Now let $a, b \geqslant 2$ be positive integers such that $(a+1)(b+1)|(q_0+1)$. Consider a tower of curves

$$X_j \xrightarrow{\phi_2} X_{j,a+1} \xrightarrow{\phi_1} X_{j,(a+1)(b+1)}.$$

Applying the construction of Section 3.3 with x_1 and x_1^{a+1} as the primitive elements of ϕ_1 and ϕ_2 respectively, we obtain the following result, proved directly from Proposition 3.3.1. We again rely on the notation $t = \dim(L(\ell Q_{\infty,j}))$, where $g_{j-1} \leqslant \ell \leqslant n_{j-1}$.

Proposition 3.7.2. *For any $j \geqslant 1$ there exists a family of H-LRC codes with parameters $[n, k, d]$ and locality $(r_1, \rho_1), (r_2, \rho_2 = 2)$, where $n = q_0^{j-1}(q_0^2 - 1), k = tab$*

$$d \geqslant n - \deg(Q_\infty)(a+1)(b+1) - q_0^{j-1}(ab + b - 2)$$

$$r_2 = a, \;\; \rho_2 = 2$$

$$r_1 = ab, \;\; \rho_1 = a + 3.$$

Note that the middle codes in this construction are optimal LRC codes, something that was not attainable with the construction of Prop. 3.7.1. Further, taking $j = 1$ in this proposition, we recover codes constructed of Prop. 3.4.1, where n is taken to be $q - 1$.

Example 3.7.3. Let $q = q_0^2$ where q_0 is a prime power and let X be the Hermitian plane curve of genus $g_0 = q_0(q_0 - 1)/2$ with the affine equation:

$$X : x^{q_0} + x = y^{q_0+1}.$$

Note that this curve coincides with the curve X_2 from the Garcia-Stichtenoth tower. The size of the evaluation set equals $q_0^3 - q_0$ which corresponds to removing the q_0 points above $0 \in \mathbb{P}^1$ on the curve. Applying the above power map construction to the case $q_0 = 8$ and $a = b = 3$ gives a Hermitian H-LRC code defined over $\mathbb{F}_{64}$. We obtain a family of codes with parameters $[n = 504, k = 9t, d]$ H-LRC code and locality $(9, 6), (3, 2)$ where:

$$d \geqslant n - 16t - 80, \;\; 1 \leqslant t \leqslant 26.$$

In particular, we obtain codes with the following parameters:

t	k	d
1	9	$408 \leqslant d \leqslant 494$
2	18	$392 \leqslant d \leqslant 478$
3	27	$376 \leqslant d \leqslant 462$
	...	
11	99	$248 \leqslant d \leqslant 334$
12	108	$232 \leqslant d \leqslant 318$
	...	

where the upper bound on d is found from (3.1).

□

3.7.3 H-LRC codes from fiber products

The result of Prop. 3.7.2 affords a generalization based on fiber products of curves. Let us recall the definition of the fiber product of curves X and Y over a curve Z. Suppose that $\phi : X \to Z$ and $\psi : Y \to Z$ are $\mathbb{k}$-covering maps. The set $X \times_Z Y := \{(x, y) \in X \times Y | \phi(x) = \phi(y)\}$ is called a *fiber product* of X and Y. In general this set does not always form a smooth algebraic curve, but we assume this in our discussion below.

Consider a tower of projective smooth absolutely irreducible curves over a finite field $\mathbb{k}$

$$X \xrightarrow{\phi_2} Y \xrightarrow{\phi_1} Z$$

where as before $\deg(\phi_2) = ab$ and $\deg(\phi_1) = b$. Let us also assume that $\Bbbk(X) = \Bbbk(Z)(x)$ for some primitive element $x \in \Bbbk(X)$ that is injective on fibers of $\phi_1 \circ \phi_2$. Choose a curve C that forms a $\Bbbk$-cover of Z and such that $X \times_Z C$ and $Y \times_Z C$ are both smooth and absolutely irreducible curves. Then x is injective on the fibers of

$$X \times_Z C \to C(\cong Z \times_Z C)$$

Applying the construction of Section 3.3, we obtain the following result.

Proposition 3.7.4. *Consider codes constructed using the tower*

$$X \times_Z C \xrightarrow{\phi_2} Y \times_Z C \xrightarrow{\phi_1} C.$$

The parameters of the codes are $[n, k, d]$*, where* n *is determined by the number of totally split points on* $X \times_Z C$ *and the distance* d *satisfies the same condition as in Prop. 3.7.2. The locality parameters are* $(r_1, \rho_1), (r_2, \rho_2 = 2)$*, where*

$$r_2 = a, \;\; \rho_2 = 2$$

$$r_1 = ab, \;\; \rho_1 = a + 3.$$

The middle code has the length $(a + 1)(b + 1)$ *and is an optimal LRC code with respect to the bound* (1.3)*.*

This construction specializes to Proposition 3.7.2 with the choices X, Y and Z such that $\Bbbk(X) = \Bbbk(x_1)$, $\Bbbk(Y) = \Bbbk(x_1^{a+1})$ and $\Bbbk(Z) = \Bbbk(x_1^{(a+1)(b+1)})$, and $C = X_{j,(a+1)(b+1)}$.

Fiber products of Artin-Schreier curves, developed in [40], look especially promising for constructing H-LRC codes because they give curves with many points, including many maximal curves.

3.7.4 H-LRC Codes with availability

In this section we consider a generalization of codes with locality wherein local correction of erasures can be performed by accessing several disjoint groups of codeword's coordinates. In the literature on LRC codes (without hierarchical structure) this generalization is called the *availability problem* [6, 17, 30, 35]. Let us first define an LRC code with the availability property (and no hierarchy of recovering sets).

Definition 3.7.5. *A linear code C is LRC with locality (r, ρ) and availability τ if for every $i \in \{1, \ldots, n\}$ there are τ punctured codes $C_{i,1}, \ldots, C_{i,\tau}$ such that*

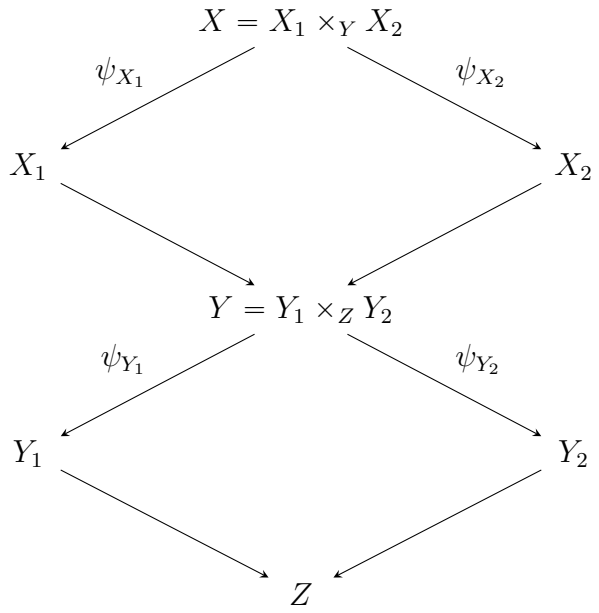
1. $\dim(C_{i,j}) \leqslant r$ *for* $j = 1, \ldots, \tau$,
2. $d(C_{i,j}) \geqslant \rho$ *for* $j = 1, \ldots, \tau$,
3. $\left|\text{supp}(C_{i,j}) \backslash \bigcup_{\substack{k \in [\tau] \\ k \neq j}} \text{supp}(C_{i,k})\right| \geqslant r$

Let us define H-LRC codes with availability.

Definition 3.7.6. *Let $\rho_2 < \rho_1$ and $r_2 \leqslant r_1$. A linear code C is H-LRC and parameters $((r_1, \rho_1), (r_2, \rho_2))$ and availability τ_1, τ_2 if it has locality (r_1, ρ_1) and availability τ_1, and each of the codes $C_{i,j}, i \in [n], j \in [\tau_1]$ is an LRC code with locality (r_2, ρ_2) and availability τ_2.*

This definition can be specialized to the case when availability is required only for local recovery at the level of the entire code C (in this case $\tau_2 = 1$), or only at the level of the middle codes (in this case $\tau_1 = 1$).

To generate H-LRC codes with availability we use a construction inspired by the LRC codes with availability introduced in [6] and developed in [17]. We focus on the example where the availability on both levels of hierarchy is $\tau_1 = \tau_2 = 2$, but the construction below can be easily extended to arbitrary availability on either level. Consider the diagram of curves given below where we assume that all the arrows correspond to separable maps between projective curves over a fixed finite field $\mathbb{k}$.



The curve Y is constructed from the fiber product of two curves of degree $s + 1$ over Z and the curve X is constructed as the fiber product of two curves of degree $r_2 + 1$ over Y. Choose a collection of c totally split fibers of the extension X/Z and let D be the set of n points in those fibers on X. The size of D equals $n = c(r_2 + 1)^2(s + 1)^2$.

Choose a positive divisor Q_∞ of degree t on Z with $L(Q_\infty) = \text{span}\{f_1, \ldots, f_m\}$ and choose primitive elements x_1, x_2, y_1, and y_2 such that $\Bbbk(X_i) = \Bbbk(Y)(x_i)$ and $\Bbbk(Y_i) = \Bbbk(Z)(y_i)$, $i = 1, 2$. Assume that the degrees of x_1, x_2 considered as maps from X to $\mathbb{P}^1$ are $h_x := \deg(x_1) = \deg(x_2)$ and the degrees of y_1, y_2 as maps from Y to $\mathbb{P}^1$ are $h_y := \deg(y_1) = \deg(y_2)$. Define h'_x to be the largest multiplicity x_i can take on a fiber of either of the maps $X \to Y_i, i = 1, 2$ (this is similar to $\deg_\psi(x)$ defined before Proposition 3.3.1). Let V be the space of functions given by

$$V = \text{span}\{f_i x_1^{j_1} x_2^{j_2} y_1^{k_1} y_2^{k_2} \mid i = 1, \ldots, m; j_1, j_2 = 0, \ldots, r_2 - 1; k_1, k_2 = 0, \ldots, s - 1\}.$$

Define the code $\mathcal{C}$ as the image of the evaluation map

$$\begin{aligned} \text{ev}: V &\to K^n \\ f &\mapsto (f(P_i) | P_i \in D). \end{aligned}$$

The properties of the code C are collected in the following proposition which follows directly from the construction.

Proposition 3.7.7. *Assume that Z is an absolutely irreducible smooth curve. The code $\mathcal{C}$ is an $[n, k, d]$ H-LRC code with parameters*

$$n = c(r_2 + 1)^2(s + 1)^2$$

$$k = ms^2 r_2^2$$

$$d \geqslant n - t(s + 1)^2(r_2 + 1)^2 - 2h_y(s - 1)(r_2 + 1)^2 - 2h_x(r_2 - 1),$$

availability 2*, and locality*

$$r_1 = r_2^2 s$$

$$\rho_1 \geqslant \max\{(r_2+1)^2(s+1) - (s-1)(r_2+1)^2 - 2h'_x(r_2-1), 8\}. \tag{3.19}$$

A middle code in this construction is obtained by restricting $\mathcal{C}$ *to a fiber of either of* $X \to Y_i, i = 1, 2$ *and is itself an H-LRC(2) code with locality parameters* $(r_2, 2)$.

3.7.5 Example: an H-LRC code with availability $\tau_1 = \tau_2 = 2$

Let $\Bbbk = \mathbb{F}_q$ be a finite field and let s, m be such that $(s+1)m = q-1$. Let $Z = \mathbb{P}^1_{\Bbbk}$ with function field $\Bbbk(z)$ and let $Y_1, \ldots, Y_4$ be curves over $\Bbbk$ with function fields $\Bbbk(z, y_1), \ldots, \Bbbk(z, y_4)$ respectively, where

$$y_i^{s+1} = z, \quad i = 1, \ldots, 4.$$

Let $Y = Y_1 \times_Z Y_2$ and let $X_1 = Y \times_Z Y_3$, $X_2 = Y \times_Z Y_4$, and $X = X_1 \times_Y X_2$. These objects fit the diagram above with all the arrows being the natural separable projections. We apply the above construction to this set of curves with $Q_\infty = t\infty_Z$ and D equal to the $m(s+1)^4$ points in $X(\Bbbk)$ above the m values in $\Bbbk$ that are $(s+1)$st powers. This gives the following result.

Proposition 3.7.8. *There exist H-LRC codes over* $\Bbbk = \mathbb{F}_q$ *with availability* $\tau_1 = \tau_2 = 2$

and code parameters

$$n = m(s+1)^4$$

$$k = t(s-1)^4$$

$$d \geqslant n - t(s+1)^4 - 4(s-1)(s+1)^2$$

and locality parameters $(s^3, 8), (s, 2)$.

All the parameters in this proposition are found directly from Proposition 3.7.7. We note that the bound on the distance ρ_1 is 8 because h'_x is $(s+1)^2$, and the first term under the maximum in (3.19) trivializes.

3.8 Asymptotic parameters

In this section we consider asymptotic parameters of H-LRC codes. In the setting that we adopt, the code length $n \to \infty$, and we call the codes asymptotically good if the limits of the rate $R := (1/n) \log_q |C|$ and relative distance $\delta := d/n$ both are bounded away from 0 as $n \to \infty$. The parameters of the middle code $[\nu, r_1, \rho_1]$ are constant and do not depend on n.

3.8.1 Asymptotically good families of H-LRC codes

Let us compute the asymptotics of the code parameters in Prop. 3.7.1. Recall that $g_j \leqslant \frac{n_j}{q_0-1}$ [10]. We have

$$\begin{aligned}\frac{d}{n}+\frac{k}{n}\frac{q_0^2}{(q_0-1)^2} &= 1-\frac{2(q_0-2)}{q_0^2-1}-\frac{q_0^2 g_j}{n}+\frac{q_0^2}{n}\\ &\geqslant 1-\frac{3}{q_0+1}+\frac{q_0^2}{n}. \end{aligned} \tag{3.20}$$

We obtain the following code family.

Proposition 3.8.1. *Let $q=q_0^2$. There exists a family of linear q-ary 2-level H-LRC codes with locality $(((q_0-1)^2,\rho_1),(q_0-1,2))$, where ρ_1 satisfies the bound of Proposition 3.7.1, and such that the rate and relative distance satisfy the inequality*

$$R \geqslant \Big(\frac{q_0-1}{q_0}\Big)^2\Big(1-\delta-\frac{3}{q_0+1}\Big). \tag{3.21}$$

The bound (3.21) is obtained by letting $j\to\infty$ and passing to the limit in (3.20).

To add flexibility to the parameters of the code family, we can decrease the maximum degrees of x,y in the functions in (3.3) from $s-1$ to $s'-1$ and from r_2-1 to $r_2'-1$, where $2\leqslant s', r_2' \leqslant q_0-1$. This gives the following extension of Proposition 3.8.1.

Proposition 3.8.2. *There exists a family of linear q-ary 2-level H-LRC codes with locality*

$$((r_1=r_2 s,\rho_1),(r_2,\rho_2=q_0+1-r_2)),\quad 2\leqslant s, r_2\leqslant q_0-1$$

and

$$R \geqslant \frac{sr_2}{q_0^2}\Big(1-\delta-\frac{q_0+s+r_2-1}{q_0^2-1}\Big).$$

Observe that, while the code families in the previous two propositions are asymptotically good, the distance of the middle codes ρ_1 does not have an explicit expression. This can be remedied by using the code family of Proposition 3.7.2, and performing a calculation similar to (3.20). We obtain the following theorem which gives a fully explicit set of parameters for an asymptotically good family of H-LRC codes.

Theorem 3.8.3. *Let $q = q_0^2$ and suppose that $\nu := (a+1)(b+1)|(q_0+1)$. There exists a family of linear q-ary 2-level H-LRC codes with locality $(r_1 = ab, \rho_1 = a+3), (r_2 = a, \rho_2 = 2))$ and the rate and relative distance satisfying the asymptotic bound*

$$R \geqslant \frac{ab}{(a+1)(b+1)}\Big(1-\delta-\frac{q_0+ab+b-1}{q_0^2-1}\Big). \tag{3.22}$$

The $[\nu, r_1, \rho_1]$ middle codes in the construction are distance-optimal in that they satisfy the bound (1.4) *with equality.*

Proof. From Proposition 3.7.2 we obtain:

$$\frac{d}{n}+\frac{k}{n}\frac{(a+1)(b+1)}{ab} \geqslant 1-\frac{ab+b-2}{q_0^2-1}-\frac{(g_Z-1)(a+1)(b+1)}{n} \tag{3.23}$$

where g_Z is the genus of the curve $X_{j,(a+1)(b+1)}$. Recalling the Riemann-Hurwitz formula

[38, p.102], we obtain the relation $g_j \geqslant 1 + (a+1)(b+1)(g_Z - 1)$, which gives

$$\frac{(g_Z - 1)(a+1)(b+1)}{n} \leqslant \frac{g_j - 1}{n}$$

Substituting this (3.23), we continue as follows:

$$\frac{d}{n} + \frac{k}{n}\frac{(a+1)(b+1)}{ab} \geqslant 1 - \frac{ab+b-2}{q_0^2 - 1} - \frac{g_j - 1}{n}$$

Since $\frac{g_j}{n} \to \frac{1}{q_0 - 1}$, we obtain (3.22) upon rearranging. □

To get an idea of the bound (3.22), assume that $a = b \approx q_0$. Assuming large q_0 and ignoring small terms, we find that the right-hand side of (3.22) is approximately $1 - \delta - \frac{2}{\sqrt{q}}$ and is in fact better than the bound (3.21).

3.8.2 A random coding argument

As in [6], let us also compute a bound on the set of achievable pairs (R, δ) obtained by a random coding argument, calling it a Gilbert-Varshamov (GV) type bound. Consider a sequence of q-ary H-LRC codes $C^{(i)}$ of length n_i with locality $((r_1, \rho_1), (r_2, \rho_2))$. Suppose that d_i is the distance of the code $C^{(i)}$ and let $\frac{d_i}{n_i} \to \delta$ as $i \to \infty$.

Proposition 3.8.4. (GV BOUND) *Assume that there exists a q-ary $[\nu, r_1, \rho_1]$ linear LRC code $\mathcal{D}$ with locality (r_2, ρ_2) and let $B_{\mathcal{D}}(s)$ be the weight enumerator of the code $\mathcal{D}$. For*

any $R > 0, \delta > 0$ *that satisfy the inequality*

$$R < \frac{r_1}{\nu} - \min_{s>0} \Big(\frac{1}{\nu} \log_q B_{\mathcal{D}}(s) - \delta \log_q s \Big), \tag{3.24}$$

there exists a sequence of H-LRC codes with asymptotic rate R *and relative distance* δ.

Proof. The ideas in the following calculation extend the approach to a Gilbert-Varshamov bound for LRC codes derived in [6, 36], so we only outline the argument. Let C be an $[n, k = Rn, d = \delta n]$ linear H-LRC code with locality parameters $\boldsymbol{r} = ((r_1, \rho_1), (r_2, \rho_2))$ as given in Def. 3.2.1. Its parity-check matrix can be taken in the form $H = (H_1|H_0)^T$, where the submatrices are as follows. The part H_1 is a block-diagonal matrix with blocks given by the parity-check matrix of the code $\mathcal{D}$. The matrix H_0 is formed of random uniform independent elements of the field $\mathbb{F}_q$ chosen independently of each other. The matrix H_1 contains $n(\nu - r_1)/\nu$ rows and the matrix H_0 contains $n\frac{r_1}{\nu} - k$ rows.

The number of vectors of weight $w = 1, \ldots, n$ in the null space of H_1 is given by $\min_{s>0} s^{-w} B_{\mathcal{D}}(s)^{n/\nu}$, and the probability that each of them is also in the null space of H_0 is $q^{-n(\frac{r_1}{\nu} - R)}$. By the union bound,

$$P(d_{\min}(C) \leqslant \delta n) = \delta n q^{-n(\frac{r_1}{\nu} - R)} \min_{s>0} s^{-w} B_{\mathcal{D}}(s)^{n/\nu}.$$

If this probability is less than one, there exist codes with distance $d_{\min} \geqslant \delta n$. Upon taking logarithms, we now obtain (3.24). □

Numerical comparison of the bounds obtained above, including (3.22) and (3.21), with

the GV bound is difficult because (3.24) is not easy to compute. Indeed, we need to find the weight distribution of the code $\mathcal{D}$ (for instance, a code in the family constructed in [35], see Sec. 1.3.2); however this is not easy even for moderate values of q_0. It is possible to replace (3.24) with a weaker bound by observing that the codes of [35] are subcodes of certain Reed-Solomon codes (more specifically, a q-ary $[\nu, r_1, \rho_1]$ code $\mathcal{D}$ is a subcode of the $[\nu, \nu - \rho_1 + 1, \rho_1]$ RS code), and therefore, their weight distributions are bounded above by the weight distribution of RS codes for which an explicit expression is available. Thus, we can use this expression to evaluate a lower estimate for the right-hand side of (3.24). Following this route, we have computed numerical examples, observing that (3.22) indeed improves upon this version of the GV bound. One such example is as follows.

Let $q_0 = 19, a = 3, b = 4$, then $\nu = 20, r_1 = 12, \rho_1 = 6$. Using the weight numerator of the $[20, 15, 6]$ RS code over $\mathbb{F}_{19^2}$ on the right-hand side of (3.24), we find that rate $R = 0.198$ is attainable for the relative distance $\delta = 0.5$. For the same δ the bound (3.22) produces a higher value $R \geqslant 0.243$.

We note again that this example does not imply that the bound (3.22) improves upon the actual GV bound which even for the above parameters is not easily computable.

3.9 Further Questions

In this chapter we applied the new general construction from Section 3.3 to several situations that result in maps between curves that fit the diagram in Equation 3.2. This includes

quotients of curves by subgroups of automorphisms and projection maps between curves in the Garcia-Stichtenoth tower. There are several directions to go from where this chapter leaves off.

- For the examples generated from quotients of Kummer curves, we are taking a quotient by very specific subgroups of automorphisms that come from the Galois action on the curves. For some of these curves, especially in the Suzuki case, the automorphism groups are much larger leaving the opportunity for various quotients of the these curve as possibilities.

- The construction discussed in this chapter comes with strict divisibility requirements for both k and n in that we have $r_2 + 1|n$ and $r_1|k$, $r_2|k$. Similar restrictions existed for algebraic construction of LRC codes as well. Paper [21] gives alternate constructions of LRC codes which are optimal and no longer require a divisibility requirement on n. It is natural to ask whether the divisibility requirements can be lifted in the HLRC codes.

- Similarly to the previous problem, it is also natural to ask how long optimal HLRC codes can possibly be. We know MDS codes cannot be longer than $2q$, as shown in [15], they show that for LRC codes the maximum length of the code is bound by roughly $O(dq^3)$.

- For additional asymptotic results, there are many candidates for other infinite towers of curves that could be examined for asymptotically good H-LRC codes. In [7], techniques are given for obtaining good towers of function fields.

Bibliography

[1] M. AALTONEN, *Notes on the asymptotic behavior of the information rate of block codes*, IEEE Trans. Inform. Theory, 30 (1984), pp. 84–85.

[2] S. BALLENTINE AND A. BARG, *Codes on curves with hierarchical locality*, in Proc. 2018 IEEE Interational Symposium on Information Theory (ISIT), Vail, CO, 2018, pp. 1201–1205.

[3] S. BALLENTINE, A. BARG, AND S. VLĂDUŢ, *Codes with hierarchical locality from covering maps of curves*. Preprint arXiv:1807.05473, 2018.

[4] A. BARG, K. HAYMAKER, E. HOWE, G. MATTHEWS, AND A. VÁRILLY-ALVARADO, *Locally recoverable codes from algebraic curves and surfaces*, in Algebraic Geometry for Coding Theory and Cryptography, E. Howe, K. Lauter, and J. Walker, eds., Springer, 2017, pp. 95–126.

[5] A. BARG, I. TAMO, AND S. VLĂDUŢ, *Locally recoverable codes on algebraic curves*, in 2015 IEEE International Symposium on Information Theory (ISIT), IEEE, 2015, pp. 1252–1256.

[6] ——, *Locally recoverable codes on algebraic curves*, IEEE Trans. Inform. Theory, 63 (2017), pp. 4928–4939.

[7] A. BASSA, P. BEELEN, AND N. NGUYEN, *Good towers of function fields*, Arxiv:1309.4951, (2013).

[8] A. DIMAKIS, P. GODFREY, Y. WU, W. M.J., AND K. RAMCHANDRAN, *Network coding for distributed storage systems*, IEEE Trans. Inform. Theory, 56 (2010), p. 4539–4551.

[9] THE GAP GROUP, *GAP – Groups, Algorithms, and Programming, Version 4.8.6*, 2016.

[10] A. GARCIA AND H. STICHTENOTH, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. math., 121 (1995), pp. 211–222.

[11] O. GEIL, *On codes from norm–trace curves*, Finite Fields and Their Applications, 9 (2003), pp. 351–371.

[12] M. GIULIETTI AND G. KORCHMÁROS, *A new family of maximal curves over a finite field*, Math. Ann., 343 (2009), pp. 229–245.

[13] P. GOPALAN, C. HUANG, H. SIMITCI, AND S. YEKHANIN, *On the locality of codeword symbols*, IEEE Trans. Inform. Theory, 58 (2012), pp. 6925–6934.

[14] V. D. GOPPA, *Codes on algebraic curves*, Dokl. Akad. Nauk SSSR, 259 (1981), pp. 1289–1290.

[15] V. GURUSWAMI, C. XING, AND Y. C., *How long can optimal locally repairable codes be?*, arxiv:1807.01064, (2018).

[16] J. HANSEN AND H. STICHTENOTH, *Group codes on certain algebraic curves with many rational points*, Appl. Alg. Commun. Contr. Comput., 1 (1990), pp. 67–77.

[17] K. HAYMAKER, B. MALMSKOG, AND G. L. MATTHEWS, *Locally recoverable codes with availability $t \geqslant 2$ from fiber products of curves*, Advances in Mathematics of Communications, 12 (2018), pp. 317–336.

[18] P. HUANG, E. YAAKOBI, AND P. SIEGEL, *Multi-erasure locally recoverable codes over small fields*. arXiv1709.09970.

[19] L. JIN, L. MA, AND C. XING, *Construction of optimal locally repairable codes via automorphism groups of rational function fields*, 2017. arXiv:1710.09638.

[20] G. M. KAMATH, N. PRAKASH, V. LALITHA, AND P. V. KUMAR, *Codes with local regeneration and erasure correction*, IEEE Trans. Inform. Theory, 60 (2014), pp. 4637–4660.

[21] O. KOLOSOV, A. BARG, I. TAMO, AND G. YADGAR, *Optimal lrc codes for all lengths $n \leqslant q$*, Arxiv:1802.00157, (2018).

[22] X. LI, L. MA, AND C. XING, *Construction of asymptotically good locally repairable codes via automorphism groups of function fields*, 2017. arXiv:1711.07703.

[23] ——, *Optimal locally repairable codes via elliptic curves*, 2017. arXiv:1712.03744.

[24] J. LIU, S. MESNAGER, AND L. CHEN, *New constructions of optimal locally recoverable codes via good polynomials*, IEEE Trans. Inform. Theory, 64 (2018), pp. 889–899.

[25] Y. LUO, C. XING, AND C. YUAN, *Optimal locally repairable codes of distance 3 and 4 via cyclic codes*. arXiv:1801.03623, 2018.

[26] J. MA AND G. GE, *Optimal binary linear locally repairable codes with disjoint repair groups*. arXiv:1711.07138.

[27] F. J. MACWILLIAMS AND N. J. A. SLOANE, *The Theory of Error-Correcting Codes*, North-Holland Publishing Co., Amsterdam e.a., 1977.

[28] Y. MANIN, *What is the maximum number of points on a curve over $\mathbb{F}_2$?*, J. Fac. Sci. Univ. Tokyo Sec. IA Math., 28 (1981), pp. 715–720.

[29] M. MOISIO, *A construction of a class of maximal Kummer curves*, Finite Fields and Their Applications, 11 (2004), pp. 667–673.

[30] A. S. RAWAT, D. S. PAPAILIOPOULOS, A. G. DIMAKIS, AND S. VISHWANATH, *Locality and availability in distributed storage*, IEEE Transactions on Information Theory, 62 (2016), pp. 4481–4493.

[31] B. SASIDHARAN, G. K. AGARWAL, AND P. V. KUMAR, *Codes with hierarchical locality*, in Proc. IEEE Int. Sympos. Inform. Theory (ISIT), Hong Kong, 2015, pp. 1257–1261. (expanded version arXiv:1501.06683).

[32] N. SILBERSTEIN, A. S. RAWAT, O. KOYLUOGLU, AND S. VISHWANATH, *Optimal locally repairable codes via rank-metric codes*, in Proc. IEEE Int. Sympos. Inform. Theory, Boston, MA, 2013, pp. 1819–1823.

[33] J. SILVERMAN, *The Arithmetic of Elliptic Curves*, vol. 254 of Graduate Texts in Mathematics, Springer, 2009.

[34] H. STICHTENOTH, *Algebraic Function Fields and Codes*, Springer, Berlin e.a., 2009.

[35] I. TAMO AND A. BARG, *A family of optimal locally recoverable codes*, IEEE Trans. Inform. Theory, 60 (2014), pp. 4661–4676.

[36] I. TAMO, A. BARG, AND A. FROLOV, *Bounds on the parameters of locally recoverable codes*, IEEE Trans. Inform. Theory, 62 (2016), pp. 3070–3083.

[37] I. TAMO, D. S. PAPAILIOPOULOS, AND A. G. DIMAKIS, *Optimal locally repairable codes and connections to matroid theory*, IEEE Trans. Inform. Theory, 62 (2016), pp. 6661–6671.

[38] M. TSFASMAN, S. VLĂDUŢ, AND D. NOGIN, *Algebraic geometric codes: Basic notions*, vol. 139 of Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI, 2007.

[39] M. TSFASMAN, S. VLĂDUŢ, AND Z. T.H., *Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound*, Math. Nachr., 108 (1982), pp. 21–28.

[40] G. VAN DER GEER AND M. VAN DER VLUGT, *Fibre products of Artin-Schreier curves and generalized Hamming weights of codes*, Journal of Combinatorial Theory, Ser. A, 70 (1995), pp. 337–348.