Codes from norm-trace curves: local recovery and fractional decoding

Aidan W. Murphy

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

Doctor of Philosophy
in
Mathematics

Gretchen L. Matthews, Chair
Felice Manganiello
Constantin L. Mihalcea
Travis W. Morrison

March 15, 2022
Blacksburg, Virginia

Keywords: algebraic geometry code, locally recoverable code, fractional decoding,
norm-trace curve

Codes from norm-trace curves: local recovery and fractional decoding

Aidan W. Murphy

(ABSTRACT)

Codes from curves over finite fields were first developed in the late 1970's by V. D. Goppa and are known as algebraic geometry codes. Since that time, the construction has been tailored to fit particular applications, such as erasure recovery and error correction using less received information than in the classical case. The Hermitian-lifted code construction of López, Malmskog, Matthews, Piñero-González, and Wootters (2021) provides codes from the Hermitian curve over $\mathbb{F}_{q^2}$ which have the same locality as the well-known one-point Hermitian codes but with a rate bounded below by a positive constant independent of the field size. However, obtaining explicit expressions for the code is challenging.

In this dissertation, we consider codes from norm-trace curves, which are a generalization of the Hermitian curve. We develop norm-trace-lifted codes and demonstrate an explicit basis of the codes. We then consider fractional decoding of codes from norm-trace curves, extending the results obtained for codes from the Hermitian curve by Matthews, Murphy, and Santos (2021).

Codes from norm-trace curves: local recovery and fractional decoding

Aidan W. Murphy

(GENERAL AUDIENCE ABSTRACT)

Coding theory focuses on recovering information, whether that data is corrupted and changed (called an error) or is simply lost (called an erasure). Classical codes achieve this goal by accessing all received symbols. Because long codes, meaning those with many symbols, are common in applications, it is useful for codes to be able to correct errors and recover erasures by accessing less information than classical codes allow. That is the focus of this dissertation. Codes with locality are designed for erasure recovery using fewer symbols than in the classical case. Such codes are said to have locality r and availability s if each symbol can be recovered from s disjoint sets of r other symbols. Algebraic curves, such as the Hermitian curve or the more general norm-trace curves, offer a natural structure for designing codes with locality. This is done by considering lines intersected with the curve to form repair groups, which are sets of $r+1$ points where the information from one point can be recovered using the rest of the points in the repair group.

An error correction method which uses less data than the classical case is that of fractional decoding. Fractional decoding takes advantage of algebraic properties of the field trace to correct errors by downloading only a λ-proportion of the received information, where $\lambda < 1$. In this work, we consider a new family of codes resulting from norm-trace curves, and study their locality and availability, as well as apply the ideas of fractional decoding to these codes.

Acknowledgments

First and foremost, I want to give a huge thank you to my advisor Gretchen Matthews, for her patience and guidance throughout my graduate career and development as a researcher, for asking me to join her when moving from Clemson University to Virginia Tech, and for being someone I always enjoy talking to, be it about interesting mathematics or anything else. I also thank my committee members for taking the time to read my drafts, and for the feedback they have provided in an effort to make this a quality dissertation.

I'm thankful for the important teachers I have had along the way. Thank you to Kevin James from Clemson, for two semesters and a summer of algebra classes that provided much challenge and pushed me to work hard towards understanding algebra. Thank you to so many professors from the numerous classes I took at S.U.N.Y. Geneseo, specifically to Chris Leary, Doug Baldwin, and Gary Towsley, who wrote my recommendation letters, and each had me almost every semester of junior and senior year in their classes.

Regarding teachers, a last and very special thank-you to Luke Martin, whose geometry class at Fairport High School set me on the path that led me where I am today.

Thank you to all the friends I have made along the way, at Geneseo, Clemson, and Virginia Tech. A special thank you to my best friend Walter Gerych, for being someone I can always talk to about anything, no matter how long it's been.

Thank you to my friend and partner Marcie Tiraphatna, for her immense support during our time at Virginia Tech, and for being someone I can confidently start to build a life with.

Lastly, thank you to everyone in my family and step-family who have supported me for as long as they have known me, especially to my parents Jim and Christine, who have known me and been there for me all my life.

Contents

List of Figures

List of Tables

List of Algorithms

List of Abbreviations

AG Algebraic geometry

HLC Hermitian-lifted code

IRS Interleaved Reed-Solomon

LRC Locally recoverable code

MDS Maximum distance separable

NTLC Norm-trace-lifted code

RS Reed-Solomon

SLC Suzuki-lifted code

Chapter 1

Introduction

The rise of Reed-Solomon codes used in applications over the past half century, along with the work of V. D. Goppa [12] which allows constructions of codes over more general algebraic curves, has lead to a wide area of research in coding theory. While the standard parameters of these codes and algorithms are still of interest, newer concepts such as locality and availability are more relevant in some settings. This focus is due to the application of codes from algebraic geometry in areas such as distributed storage and other big data applications, where being able to correct errors or recover erasures by accessing less data is often advantageous. Locality and availability began to be investigated in the early 2010s [10, 11, 29].

We will see that locality and availability may arise naturally from the intersection of lines with algebraic curves. The intersection of lines with the Hermitian curve is utilized in the lifting procedure of [18], where Hermitian-lifted codes are defined and studied. The Hermitian-lifted codes are interesting because they retain the natural locality of one-point Hermitian codes, while also having the property of their rate being bounded below by a constant independent of the field size. This lower bound on the rate in essence means that the inefficiency of the codes has a fundamental upper bound. Despite these results, the codes themselves lack explicit expression, as the relevant monomials are yet to be classified.

Norm-trace curves are a generalization of the Hermitian curves. Algebraic geometry codes have been constructed from them [9], offering some improvements over Hermitian codes in terms of relative distance or rate. Here we consider these curves in the construction similar

to Hermitian-lifted codes and investigate the properties of the resulting codes. We show that these norm-trace-lifted codes are distinct from other constructions in the literature, and that norm-trace-lifted codes are advantageous over Hermitian-lifted codes in several ways.

Locally recoverable codes such as the Hermitian-lifted codes, offer the advantage of recovering data with less information than is classically needed by downloading only a subset of received symbols for recovery. Fractional decoding is a procedure for error correction that effectively downloads a fraction of the necessary information from received symbols. This goal is achieved using algebraic properties of the field trace defined over finite fields. The formulation of fractional decoding was first presented in [30], and followed by an extension to Reed-Solomon codes in [24]. Most recently, this approach was modified for a new set of codes from the Hermitian curve in collaboration with Gretchen L. Matthews and Welington Santos.

In this work we extend these results to norm-trace curves, as well as introduce ideas to improve the decoding radius for the algebraic geometry codes considered previously. The ideas for improving the decoding radius of codes from Hermitian and norm-trace curves then lead naturally to an application of fractional decoding techniques to Hermitian-lifted codes and norm-trace-lifted codes.

This document is structured as follows. In the first chapter, Sections 1.1, 1.2, and 1.3, we lay down the basic definitions relevant to algebraic function fields, algebraic curves, and coding theory. Lastly, Section 1.4 describes the algebraic geometry codes that are relevant to to this work.

The second chapter covers with norm-trace-lifted codes. Section 2.1 reviews Hermitian-lifted codes. Section 2.2 discusses the intersection cardinalities of lines with norm-trace curves. Section 2.3 then defines and develops norm-trace-lifted codes. Comparisons to other codes

are contained in Section 2.4, detailing rate, parameter, and basis monomial comparisons. Lastly for norm-trace-lifted codes, a more general result on curve-lifted codes is presented in Section 2.5, where they are specifically applied to Suzuki curves. Future research directions are contained in Section 2.6, including conjectures related to this work.

The third and final chapter describes fractional decoding, and builds towards fractional decoding of the norm-trace-lifted codes in Chapter 2. In Section 3.1 all necessary definitions are given, followed by the procedure for fractional decoding of Reed-Solomon codes. Section 3.2 contains collaborative work with Gretchen L. Matthews and Welington Santos on fractional decoding of codes from the Hermitian curve, and these results are extended to codes from the more general norm-trace curves. An improvement on these procedures involving use of alternate lines for recovery is laid out in Section 3.3 and is applied to codes from Hermitian curves while also motivating application to Hermitian-lifted codes. The application to Hermitian-lifted codes is found in Section 3.4. An analagous result for norm-trace-lifted codes is contained in Section 3.5. Future research directions and conjectures related to this work are contained in Section 3.6.

1.1 Algebraic function fields

Throughout, $\mathbb{F}_q$ denotes the finite field with q elements, where $q = p^h$ is a power of some prime p. In this section, we review the relevant definitions related to the theory of algebraic function fields. See [27] for additional details.

Definition 1.1. Let $x \in F$ be transcendental over K where F is an extension of K. The field

$$K(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], g(x) \neq 0 \right\}$$

is called the *rational function field*.

Definition 1.2. An *algebraic function field* F/K of one variable over K is an extension field $F \supseteq K$ such that F is a finite algebraic extension of the rational function field $K(x)$ for some element $x \in F$ which is transcendental over K.

The following are examples of algebraic function fields.

Example 1.3. Let $H = \mathbb{F}_{q^2}(x, y)$ where x and y are related by

$$y^q + y = x^{q+1}.$$

The extension $H/\mathbb{F}_{q^2}$ is known as the *Hermitian function field*.

For the next example, we need to define the field norm and trace with respect to the field extension $\mathbb{F}_{q^r}/\mathbb{F}_q$.

Definition 1.4. The *norm* of $\alpha \in \mathbb{F}_{q^r}$ with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ is

$$N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = \alpha^{\frac{q^r-1}{q-1}}.$$

The *trace* of $\alpha \in \mathbb{F}_{q^r}$ with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ is

$$\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = \sum_{i=0}^{r-1} \alpha^{q^i}.$$

It is well-known that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha), \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$ for any $\alpha \in \mathbb{F}_{q^r}$.

Example 1.5. Let $F = \mathbb{F}_{q^r}(x, y)$ where x and y are related by

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

The extension $F/\mathbb{F}_{q^r}$ is known as the *norm-trace function field*, since $y^{q^{r-1}} + \cdots + y$ can be seen as the trace of y relative to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$, and $x^{\frac{q^r-1}{q-1}}$ can be seen as the norm of x relative to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$. Note that taking $r = 2$ gives the Hermitian function field.

As we will see, the Hermitian function field is of particular importance in the construction of codes. We now proceed to the definition of a divisor, and subsequently the Riemann-Roch space corresponding to a divisor.

Definition 1.6. A *valuation ring* of the function field F/K is a ring $\mathcal{O} \subseteq F$ with the following properties:

1. $K \subsetneq \mathcal{O} \subsetneq F$, and
2. for every $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

Definition 1.7. A *place* P of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K. Denote the set of places of F/K as $\mathbb{P}_F$.

Definition 1.8. Let $P \in \mathbb{P}_F$.

1. The *residue class field* of P is $F_P \coloneqq \mathcal{O}_P/P$. The map $x \mapsto x(P)$ from F to $F_p \cup \{\infty\}$ is called the *residue class map* with respect to the place P.
2. The *degree* of P is $\deg P \coloneqq [F_P : K]$. A place of degree one is also called *rational place* of F/K.

Definition 1.9. A *discrete valuation* of F/K is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:

1. $v(f) = \infty$ if and only if $f \equiv 0$.

2. $v(fg) = v(f) + v(g)$ for all $f, g \in F$.

3. $v(f+g) \geq \min\{v(f), v(g)\}$ for all $f, g \in F$.

4. There exists an element $h \in F$ with $v(h) = 1$.

5. $v(a) = 0$ for all $0 \neq a \in K$.

Definition 1.10. The *divisor group* of F/K, denoted $\mathrm{Div}(F)$, is the free abelian group on the places of F/K. The elements of $\mathrm{Div}(F)$ are called *divisors* of F/K; in other words, a divisor is a formal sum

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ with } n_P \in \mathbb{Z} \text{ and } n_P = 0 \text{ for almost all } P \in \mathbb{P}_F.$$

The *support of* D is defined as

$$\mathrm{supp}(D) \coloneqq \{P \in \mathbb{P}_F \mid n_P \neq 0\}.$$

It will be convenient to write

$$D = \sum_{P \in S} n_P P$$

where $S \subseteq \mathbb{P}_F$ is a finite set with $S \supseteq \mathrm{supp}(D)$.

Definition 1.11. For a rational function $h(x) = \frac{f(x)}{g(x)}$, the α where $f(\alpha) = 0$ and $g(\alpha) \neq 0$ are called the *zeros* of $h(x)$, and the α where $g(\alpha) = 0$ are called the *poles* of $h(x)$.

Definition 1.12. Let $0 \neq f \in F$ and denote by Z (resp. N) the set of zeros (resp. poles) of f in $\mathbb{P}_F$. Then we define:

$$(f)_0 \coloneqq \sum_{P \in Z} v_P(f) P, \text{ the zero divisor of } f,$$

$$(f)_\infty \coloneqq \sum_{P \in N} (-v_P(f))P, \text{ the pole divisor of } f,$$

and

$$(f) \coloneqq (f)_0 - (f)_\infty, \text{ the principal divisor of } f.$$

Definition 1.13. For divisors

$$D_1 = \sum_{P \in \mathbb{P}_F} n_P P \text{ and } D_2 = \sum_{P \in \mathbb{P}_F} m_P P,$$

we write $D_1 \geq D_2$ if $n_P \geq m_P$ for all $P \in \mathbb{P}_F$.

Definition 1.14. For a divisor $D \in \mathrm{Div}(F)$, the *Riemann-Roch space* associated with D is

$$\mathcal{L}(D) \coloneqq \{f \in F \mid (f) \geq -D\} \cup \{0\}.$$

In later sections, we often take D to be effective, meaning $D > 0$, i.e.

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ with } n_P \geq 0 \text{ for all } P \in \mathbb{P}_F.$$

In that case, the divisor D can be considered as a pole allowance; that is, the functions in $\mathcal{L}(D)$ are those which have poles of order no more than n_P at each point P in the support of the divisor D.

Example 1.15. Consider the rational function field $\mathbb{F}_q(x)/\mathbb{F}_q$. For the divisor $D = mP_\infty$ where P_∞ is the infinite place, the Riemann-Roch space associated to D is the set of polynomials $f(x)$ which have degree $\deg(f) \leq m$.

Example 1.16. [26] Let $H/\mathbb{F}_q$ be the Hermitian function field. For the divisor $D = mP_\infty$, where P_∞ is the infinite place, the Riemann-Roch space is generated by a set of monomials

$x^a y^b$ which have poles of order no more than m at P_∞. More precisely, the space $\mathcal{L}(D)$ is generated by monomials $x^a y^b$ where

$$aq + b(q+1) \leq m.$$

Lastly, we build toward the definition of genus of function fields, which will also describe the genus of the algebraic curves which correspond to the function fields.

Definition 1.17. The *degree* of a divisor D is defined as

$$\deg(D) \coloneqq \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \deg(P).$$

Definition 1.18. For $D \in \mathrm{Div}(F)$, the integer $\ell(D) \coloneqq \dim \mathcal{L}(D)$ is called the *dimension* of the divisor D.

Remark 1.19. [27] For each divisor $D \in \mathrm{Div}(F)$, the space $\mathcal{L}(D)$ is a finite-dimensional vector space over K. More precisely, if $D = D_+ - D_-$ with disjoint effective divisors D_+ and D_-, where the components of D_+ denote poles and the components of D_- denote zeros, then

$$\ell(D) \leq \deg(D_+) + 1.$$

Definition 1.20. The *genus* g of F/K is defined by

$$g \coloneqq \max\{\deg(D) - \ell(D) + 1 : D \in \mathrm{Div}(F)\}.$$

There is a result bounding the number of rational places that a function field with genus g may have, called the Hasse-Weil bound. The Hasse-Weil bound will become relevant in algebraic geometry codes because of the correspondence between rational places and rational

points on an algebraic curve.

Theorem (Hasse-Weil bound)**.** The number $N = N(F)$ of places of $F/\mathbb{F}_q$ of degree one satisfies the inequality

$$|N - (q+1)| \leq 2gq^{1/2},$$

where g is the genus of the function field $F/\mathbb{F}_q$.

We finish this section with definitions that are relevant to other constructions of codes from norm-trace curves.

Definition 1.21. An *adele* of F/K is a mapping

$$\alpha : \begin{cases} \mathbb{P}_F \longrightarrow F, \\ P \longmapsto \alpha_P, \end{cases}$$

such that $\alpha_P \in \mathcal{O}_P$ for almost all $P \in \mathbb{P}_F$. We regard an adele as an element of the direct product $\Pi_{P\in\mathbb{P}_F} F$ and therefore use the notation $\alpha = (\alpha_P)_{P\in\mathbb{P}_F}$, or even shorter as $\alpha = (\alpha_P)$. The set

$$\mathcal{A}_F \coloneqq \{\alpha : \alpha \text{ is an adele of } F/K\}$$

is called the *adele space* of F/K.

Definition 1.22. For $D \in \mathrm{Div}(F)$ we define

$$\mathcal{A}_F(D) \coloneqq \{\alpha \in \mathcal{A}_F : v_P(\alpha) \geq -v_P(D) \text{ for all } P \in \mathbb{P}_F\}.$$

Definition 1.23. A *Weil differential* of F/K is a K-linear map $\omega : \mathcal{A}_F \to K$ vanishing on $\mathcal{A}_F(D) + F$ for some divisor $D \in \mathrm{Div}(F)$. We call

$$\Omega_F \coloneqq \{\omega : \omega \text{ is a Weil differential of } F/K\}$$

the *module of Weil differentials* of F/K. For $D \in \mathrm{Div}(F)$ let

$$\Omega_F(D) \coloneqq \{\omega \in \Omega_F : \omega \text{ vanishes on } \mathcal{A}_F(D) + F\}.$$

Definition 1.24. The divisor (ω) of a Weil differential $\omega \neq 0$ is the uniquely determined divisor of F/K satisfying

1. ω vanishes on $\mathcal{A}_F((\omega)) + F$, and
2. if ω vanishes on $\mathcal{A}(D) + F$, then $D \leq (\omega)$.

A divisor W is called a *canonical divisor* of F/K if $W = (\omega)$ for some $\omega \in \Omega_F$.

We finish the background relevant to alternate code constructions with some definitions about extensions of algebraic function fields.

Definition 1.25. An algebraic function field F'/K' is called an *algebraic extension* of F/K if $F' \supseteq F$ is an algebraic field extension and $K' \supseteq K$.

Definition 1.26. Consider an algebraic extension F'/K' of F/K. A place $P' \in \mathbb{P}_{F'}$ is said to *lie over* $P \in \mathbb{P}_F$ if $P \subseteq P'$. We also say P' is an *extension of* P, or that P *lies under* P', and write $P'|P$.

Definition 1.27. Let F'/K' be an algebraic extension of F/K, and let $P' \in \mathbb{P}_{F'}$ be a place of F'/K' lying over $P \in \mathbb{P}_F$. The integer $e(P'|P) \coloneqq e$ with

$$v_{P'}(f) = e \cdot v_P(f) \text{ for all } f \in F$$

is called the *ramification index* of P' over P. We say that $P'|P$ is *ramified* if $e(P'|P) > 1$, and $P'|P$ is *unramified* if $e(P'|P) = 1$.

Definition 1.28. Let F'/K' be an extension of F/K of degree $[F' : F] = n$ and let $P \in \mathbb{P}_F$.

1. The place P *splits completely* in F'/F if there are exactly n distinct places $P' \in \mathbb{P}_{F'}$ with $P'|P$.

2. The place P is *totally ramified* in F'/F if there is a place $P' \in \mathbb{P}_{F'}$ with $P'|P$ and $e(P'|P) = n$.

1.2 Algebraic curves

Algebraic coding theory often uses the language of algebraic curves rather than function fields. Here, the term algebraic curve refers to nonsingular, absolutely irreducible, projective algebraic varieties of dimension one. In the rest of this document, we consider plane algebraic curves.

The following definitions contain important bounds relevant to algebraic curves, as well as definitions of some special classes of algebraic curves which we use to build codes (particularly, norm-trace curves).

Definition 1.29. Denote by $\mathcal{X}(\mathbb{F}_q)$ the $\mathbb{F}_q$-rational points on the curve $\mathcal{X}$.

Because of the correspondence between places of degree one in the relevant function field and rational points on the respective curve, the Hasse-Weil bound gives an upper bound on the number of $\mathbb{F}_q$-rational points on any curve $\mathcal{X}$ over $\mathbb{F}_q$, namely

$$|\mathcal{X}(\mathbb{F}_q)| \leq q + 1 + 2gq^{1/2}.$$

Definition 1.30. An algebraic curve over $\mathbb{F}_q$ whose number of $\mathbb{F}_q$-rational points meets the Hasse-Weil bound with equality is called a *maximal curve*.

We now define an important curve known as the Hermitian curve.

Definition 1.31. Let $\mathcal{X}_q$ be the projective closure of the curve defined by $x^{q+1} = y^q + y$ defined over $\mathbb{F}_{q^2}$. This curve is known as the *Hermitian curve*.

Remark 1.32. [23] The genus of the Hermitian curve is $g = \frac{q(q-1)}{2}$. The Hermitian curve is maximal with respect to the Hasse-Weil bound, since there are $q^3 + 1$ points in $\mathcal{X}_q(\mathbb{F}_{q^2})$.

We consider the Hermitian curve over $\mathbb{F}_{q^2}$ instead of $\mathbb{F}_q$ because the Hermitian curve is a maximal curve over $\mathbb{F}_{q^2}$ and is not maximal over $\mathbb{F}_q$.

Definition 1.33. The *norm-trace curve* $\mathcal{X}_{q,r}$ over $\mathbb{F}_{q^r}$ is defined by the affine equation

$$N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x) = \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y),$$

meaning

$$\mathcal{X}_{q,r} : x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + \cdots + y^q + y.$$

Remark 1.34. The norm-trace curve $\mathcal{X}_{q,r}$ with $r = 2$ gives

$$\mathcal{X}_{q,2} : x^{q+1} = y^q + y,$$

the Hermitian curve over $\mathbb{F}_{q^2}$.

The following remarks about norm-trace curves will be utilized later when defining the corresponding one-point codes and lifted codes.

Proposition 1.35. *[9] For the norm-trace curve $\mathcal{X}_{q,r}$, $|\mathcal{X}_{q,r}(\mathbb{F}_{q^r})| = q^{2r-1} + 1$. Thus, there are q^{2r-1} affine points on $\mathcal{X}_{q,r}$.*

Proof. Recall that the zeros of the norm-trace curve over $\mathbb{F}_{q^r}$ are the points (α, β) such that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$.

We claim that $\alpha = 0 \in \mathbb{F}_{q^r}$ such that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = 0$. We further claim that given $c \in \mathbb{F}_q \backslash \{0\}$ there are precisely $a = \frac{q^r-1}{q-1}$ elements $\alpha \in \mathbb{F}_{q^r}$ such that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = c$, and that given any $c \in \mathbb{F}_q$ that there are precisely $b = q^{r-1}$ elements $\alpha \in \mathbb{F}_{q^r}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = c$.

This claim can be confirmed by the fact that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}$ is a homomorphism from the multiplicative group $\mathbb{F}_{q^r} \backslash \{0\}$ to the multiplicative group $\mathbb{F}_q \backslash \{0\}$, and that $\mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}$ is a homomorphism from the additive group $\mathbb{F}_{q^r}$ to the additive group $\mathbb{F}_q$ [16, Theorem 2.23]. ■

Remark 1.36. [21] The genus of the norm-trace curve is

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

Unlike the Hermitian curve, in general, norm-trace curves are not maximal.

1.3 Linear codes

The material in the previous sections has applications in the theory of error correcting codes, which have application where data is stored or transmitted, such as CDs, DVDs, servers that store often-accessed data (such as movies on Netflix), and QR codes.

Basic definitions

Definition 1.37. A *linear code* C of length n over $\mathbb{F}_q$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$.

The elements of C are called *codewords*. Given a code C of length n, the set of indices of the codewords is $[n] \coloneqq \{1, \ldots, n\}$.

Definition 1.38. Let C be a linear code over $\mathbb{F}_q$, and $wt(c) = |\{i \in [n] \mid c_i \neq 0\}|$ be the

weight of $c \in \mathbb{F}_q^n$. We say C is an $[n, k, d]$ code if C is length n, $k = \dim_{\mathbb{F}_q}(C)$ and

$$d = \min\{wt(c) \mid c \in C \backslash \{0\}\}$$

is the *minimum distance* of C.

Definition 1.39. The *rate* of an $[n, k, d]$ code C is $\frac{k}{n}$.

The rate of a linear code measures the efficiency of the code, being the ratio of the length k of the string of data to be encoded, and the length n of the string after encoding. A code with a higher rate introduces less redundancy during the encoding process. An analagous parameter exists for the minimum distance.

Definition 1.40. The relative distance of an $[n, k, d]$ code C is $\frac{d}{n}$.

The minimum distance of a linear code satisfies the following bound.

Theorem (Singleton bound)**.** For an $[n, k, d]$ code C,

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

The Singleton bound shows that there is an inherent balance between the minimum distance and the dimension of a linear code. Any code which meets this bound with equality is called *maximum distance separable* (or MDS).

Given an $[n, k, d]$ code C over $\mathbb{F}_q$, let $w \in \mathbb{F}_q$ be a received word resulting from a sent codeword $c \in C$. We consider two situations:

1. $w = (w_1, \ldots, w_n) \in (\mathbb{F}_q^n \cup \{?\})^n$ where $w_i \in \{c_i, ?\}$ for all $i \in [n]$,
2. $w = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$ such that $d(w, c) \leq \lfloor \frac{d-1}{2} \rfloor$.

Here, the symbol ? denotes an erasure, so that

1. an erasure occurs at position i if and only if $w_i =?$,

2. an error occurs at position i if and only if $w_i \neq c_i$.

Note that positions of an erasure are known, while error positions are not apparent from w.

The goal is to determine the original codeword $c \in C$.

Proposition 1.41. *An $[n, k, d]$ linear code C is able to*

- *recover up to $d-1$ erasures, or*

- *correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.*

Proof. We follow the proofs of [13]. For each part, we consider minimum distance decoding, which is a decoding procedure defined by choosing the nearest codeword in weight to the received word.

First we prove that C can recover up to $d-1$ erasures. Let $y \in (\mathbb{F}_q^n \cup \{?\})^n$ be the received word. We claim that there is a unique $c = (a_1, \ldots, a_n) \in C$ such that $y_i = a_i$ for every i where $y_i \neq ?$. For the sake of contradiction, assume that there are two distinct codewords $c_1, c_2 \in C$ such that both c_1 and c_2 agree with y in the unerased positions. Note that this assumption implies that c_1 and c_2 agree in the positions i with $y_i \neq ?$ is not an erasure. Thus, $wt(c_1 - c_2) \leq |\{i : y_i =?\}| \leq d-1$, which contradicts the assumption that C has minimum distance d. Therefore, we may recover $d-1$ erasures in y by finding the unique codeword c_1.

Now we prove that C can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors. Let $c_1 \in C$ be the transmitted codeword

and $y \in \mathbb{F}_q^n$ be the received word. Note that

$$wt(y - c_1) \leq d.$$

Assume if y is decoded as c_2 and $c_2 \neq c_1$. Note that

$$wt(y - c_2) \leq wt(y - c_1).$$

Then,

$$wt(c_1 - c_2) \leq wt(c_2 - y) + wt(c_1 - y) \leq 2 \cdot wt(c_1 - y) \leq d - 1$$

from the triangle inequality, which implies that the minimum distance of C is at most $d-1$, a contradiction. Thus, it is possible to correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors. ■

The above bounds on erasure recovery and error correction both assume access to all other coordinates of the received word w. When the length of the code is large, this action is very inefficient. The following concepts of locality and availability address how we may recover the codeword c while accessing less information.

Locality and availability

Codes with locality allow recovery of a codeword c with much less information than is normally needed for an $[n, k, d]$ code C. Classical models for erasure recovery utilize all symbols w_i to recover the symbols c_i where $i \in [n]$, $w_i =?$. If a code has locality r, then only r other coordinates of the received word are needed to recover an erasure, instead of accessing all other coordinates.

Definition 1.42. A code $C \subseteq \mathbb{F}_q^n$ with codewords $c = (c_1, \ldots, c_n)$ has *locality* r if for all

$i \in [n]$, there exists

$$R_i \subseteq [n] \backslash \{i\}$$

where $|R_i| \leq r$ such that

$$c_i = \varphi(c\,|_{R_i})$$

for some function $\varphi : \mathbb{F}_q^r \to \mathbb{F}_q$. Additionally;

- The set R_i is called a *recovery set* for i.
- The set $\overline{R_i} \coloneqq R_i \cup \{i\}$ is called a *repair group* for i.

The parameters of an $[n, k, d]$ code C with locality r satisfy a Singleton-like bound [29]:

$$d + k \leq n + 1 - \left(\left\lceil \frac{k}{r} \right\rceil - 1 \right).$$

If the parameters of C meet this bound with equality, C is called an *optimal locally recoverable code*.

There may be instances when not all the elements in a specific recovery set will be available. Indeed, suppose $w \in \mathbb{F}_q^n$ is received and $w_i =?$. If there exists R_i such that $j \in R_i$ and $w_j =?$, then c_i may not be recovered. Having multiple recovery sets is a solution to this problem. For instance, if there exists some $R_i' \subseteq [n] \backslash \{R_i \cup \{i\}\}$ and $w_j \in \mathbb{F}_q$ for all $j \in R_i'$, then c_i may be recovered from R_i'. This feature is known as availability.

Definition 1.43. A code $C \subseteq \mathbb{F}_q^n$ has *availability* s if there exist recovery sets

$$R_{i,1}, \ldots, R_{i,s} \subseteq [n] \backslash \{i\}$$

for each $i \in [n]$ such that

$$R_{i,j} \cap R_{i,t} = \emptyset$$

for all $j \neq t$.

The condition that the sets be disjoint is meant to prevent erasures being common to several recovery sets. An $[n, k, d]$ locally recoverable code with locality r and availability s satisfies another Singleton-like bound [28]:

$$d \leq n - \sum_{i=0}^{s} \left\lfloor \frac{k-1}{r^i} \right\rfloor .$$

1.4 Algebraic geometry codes

All codes considered in this dissertation are evaluation codes. These codes are formed by taking a set of $\mathbb{F}_q$-valued functions, and evaluating those functions at a set of $\mathbb{F}_q$-rational points on a curve $\mathcal{X}$ over $\mathbb{F}_q$ where the functions have no poles. The precise definition is given next.

Definition 1.44. Let V be a set of $\mathbb{F}_q$-valued functions that may be evaluated at points $P_1, \ldots, P_n$ on a curve $\mathcal{X}$ over a finite field $\mathbb{F}_q$.

Evaluation codes have the form

$$C(D, V) \coloneqq \{(f(P_1), \ldots, f(P_n)) : f \in V\} \subseteq \mathbb{F}_q^n$$

where $D = (P_1, \ldots, P_n)$; that is, $C(D, V) = ev(V)$ where

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

In the literature, D is often expressed as a divisor $D = P_1 + \cdots + P_n$ on $\mathcal{X}$. The main examples of evaluation codes are one-point algebraic geometry (AG) codes, particularly Reed-Solomon

codes. In this work we also consider Hermitian codes and norm-trace codes.

Definition 1.45. Let $F/\mathbb{F}_q$ be an algebraic function field, $D = P_1 + \cdots + P_n$ be the sum of n distinct places of $F/\mathbb{F}_q$ of degree one, and G be a divisor with disjoint support from D. The *algebraic geometry code* (or AG code) $C_{\mathcal{L}}(D, G)$ associated with divisors D and G is defined as

$$C_{\mathcal{L}}(D, G) \coloneqq \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Definition 1.46. An algebraic geometry code $C_{\mathcal{L}}(D, G)$ where $G = mP_\infty$ for some $m \in \mathbb{Z}^+$ is called a *one-point algebraic geometry code*.

The parameters of $C_{\mathcal{L}}(D, G)$ are detailed in the following theorem.

Theorem 1.47. *[27] The algebraic geometry code $C_{\mathcal{L}}(D, G)$ is an $[n, k, d]$ code with parameters*

$$k \geq \deg(G) - g + 1,$$

$$d \geq n - \deg(G).$$

Hence, $C_{\mathcal{L}}(D, G)$ satisfies

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

Note that the code $C_{\mathcal{L}}(D, G)$ is not necessarily MDS but its parameters are at most g away from satisfying the Singleton bound with equality.

Reed-Solomon codes

Reed-Solomon codes are a family of algebraic geometry codes over the projective line $\mathbb{P}^1_{\mathbb{F}_q}$, and the functions to be evaluated are polynomials whose degrees are no more than some $k < n < q$.

Definition 1.48. Let $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_q\}$. Set positive integers $k \leq n \leq q$. Let

$$\mathbb{F}_q[x]_{<k} \coloneqq \{f \in \mathbb{F}_q[x] : \deg f < k\}.$$

The *Reed-Solomon code* $RS(q, n, k)$ is the evaluation code

$$RS(q, n, k) = \{(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) : f \in \mathbb{F}_q[x]_{<k}\} \subseteq \mathbb{F}_q^n.$$

Note that $RS(q, n, k) = \mathcal{C}_{\mathcal{L}}(D, (k-1)P_\infty)$ where P_∞ is the point at infinity on the projective line and $D = P_1 + \cdots + P_q$ is the sum of the other $\mathbb{F}_q$-rational points.

To encode a message $a = (a_0, \ldots, a_{k-1}) \in \mathbb{F}_q^k$, set

$$f_a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}.$$

Then

$$(a_0, \ldots, a_{k-1}) \mapsto (f_a(\alpha_1), f_a(\alpha_2), \ldots, f_a(\alpha_n)) \in \mathbb{F}_q^n.$$

Remark 1.49. The Reed-Solomon code $RS(q, n, k)$ is an $[n, k, n-k+1]$ code.

Proof. Set arbitrary messages $m_1 \neq m_2 \in \mathbb{F}_q^n$, and denote by $RS(m) \in \mathbb{F}_q^n$ the encoded message vector for message m. Note that $f_{m_1}(x), f_{m_2}(x) \in \mathbb{F}_q[x]$ are distinct polynomials of degree at most $k-1$. Then, $f_{m_1}(x) - f_{m_2}(x) \neq 0$ also has degree at most $k-1$. Note

$$\mathrm{wt}(RS(m_1) - RS(m_2)) = d(RS(m_1), RS(m_2)).$$

The weight of $RS(m_1) - RS(m_2) \in RS(q, n, k)$ is

$$d(RS(m_1), RS(m_2)) = n - |\{\alpha_i : f_{m_1}(\alpha_i) = f_{m_2}(\alpha_i)\}|.$$

Because $f_{m_1}(x) - f_{m_2}(x) \in \mathbb{F}_q[x]_{<k}$, it has at most $k-1$ roots. Hence, the weight of $RS(m_1) - RS(m_2)$ is at least $n-(k-1) = n-k+1$. Thus, $d \geq n-k+1$. According to the Singleton bound, $d = n-k+1$. ■

Reed-Solomon codes maximal with respect to the Singleton bound. The codes to be defined later, such as Hermitian codes, in general do not meet the Singleton bound with equality, but rather exhibit other desirable parameters.

We give a few more definitions relevant to the fractional decoding procedures detailed in Chapter 3. One object used often in Reed-Solomon error correction is the error locator polynomial.

Definition 1.50. Let C be a Reed-Solomon code, and let y be the received word from codeword $(p(\alpha_i))_{i=1}^n \in C$. An *error locator polynomial* is a polynomial $E(x)$ such that

$$E(\alpha_i) = 0 \text{ if and only if } y_i \neq p(\alpha_i).$$

Recovering an error locator polynomial means discovering the locations where errors occurred in a codeword. Lastly, fractional decoding requires understanding of interleaved Reed-Solomon codes.

Definition 1.51. Consider the Reed-Solomon codes $RS(q,n,k_i)$, $i \in [m]$ each with evaluation points $\{\alpha_1^i, \ldots, \alpha_n^i\}$. Consider the set of dimensions $\mathcal{K} = \{k_1, \ldots, k_m\}$ An *interleaved Reed-Solomon code* is the set of matrices

$$IRS(q,n,\mathcal{K},m) = \left\{ \begin{bmatrix} f_1(\alpha_1^1) & \ldots & f_1(\alpha_n^1) \\ \vdots & \ddots & \vdots \\ f_m(\alpha_1^m) & \ldots & f_m(\alpha_n^m) \end{bmatrix} : (f_i(\alpha_1^i) \ldots f_i(\alpha_n^i)) \in RS(q,n,k_i), i \in [m] \right\}.$$

Hermitian codes

Remark 1.52. [26] For the Hermitian function field $\mathbb{F}_q(x,y)$ given by $x^{q+1} = y^q + y$ and for $m \in \mathbb{Z}^+$, the Riemann-Roch space $\mathcal{L}(mP_\infty)$ is

$$\mathcal{L}(mP_\infty) = \left\langle x^a y^b : 0 \leq b \leq q-1, aq + b(q+1) \leq m \right\rangle,$$

where P_∞ is the point at infinity on $\mathcal{X}_q(\mathbb{F}_{q^2})$.

Definition 1.53. Let $\mathcal{X}_q$ be the Hermitian curve defined over $\mathbb{F}_{q^2}$.

Let P_∞ be the point at infinity on $\mathcal{X}_q(\mathbb{F}_{q^2})$, and

$$D = P_1 + \cdots + P_n$$

be a divisor supported by the $n \coloneqq q^3$ distinct $\mathbb{F}_{q^2}$-rational points on $\mathcal{X}_q$ other than P_∞.

The *one-point Hermitian code* $C(D, mP_\infty)$ is

$$C(D, mP_\infty) \coloneqq \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(mP_\infty)\} \subseteq \mathbb{F}_{q^2}^n.$$

The maximality of Hermitian curves with respect to the Hasse-Weil bound has the benefit of maximizing the length of the code, for the given genus and field size.

Proposition 1.54. *[26, 31] The one-point Hermitian code $C(D, mP_\infty)$ is a $[q^3, k, d]$ code where the minimum distance d is dependent on the dimension k.*

Let

$$A(m) = \{0 \leq \ell \leq m : \text{ there exist nonnegative } i, j \in \mathbb{Z} \text{ such that } \ell = iq + j(q+1)\},$$

and let

$$\tilde{m} = \max_{\ell}\{\ell : \ell \in A(m)\}.$$

Specifically for the codes $C(D, mP_\infty)$ *we consider with* $m \leq q^2 - 1$, *if* $\tilde{m} = aq + b$ *where* $0 \leq b \leq a \leq q - 1$,

$$k = \frac{a(a+1)}{2} + b + 1,$$

$$d = n - \tilde{m}.$$

Norm-trace codes

Remark 1.55. [9] For the norm-trace function field $\mathbb{F}_q(x, y)$ given by $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x) = \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y)$ and for $m \in \mathbb{Z}^+$, the Riemann-Roch space $\mathcal{L}(mP_\infty)$ is

$$\mathcal{L}(mP_\infty) = \left\langle x^a y^b : 0 \leq b \leq q^{r-1} - 1, aq^{r-1} + b\left(\frac{q^r - 1}{q - 1}\right) \leq m \right\rangle,$$

where P_∞ is the point at infinity on $\mathcal{X}_{q,r}(\mathbb{F}_{q^r})$.

Definition 1.56. Let $\mathcal{X}_{q,r}$ be the norm-trace curve defined by $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x) = \mathrm{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y)$ defined over $\mathbb{F}_{q^r}$.

Let P_∞ be the point at infinity in $\mathcal{X}_{q,r}(\mathbb{F}_{q^r})$, and

$$D = P_1 + \cdots + P_n$$

be a divisor supported by $n = q^{2r-1}$ distinct $\mathbb{F}_{q^r}$-rational points on $\mathcal{X}_{q,r}$ other than P_∞.

The *one-point norm-trace code* $C(D, mP_\infty)$ is

$$C(D, mP_\infty) \coloneqq \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(mP_\infty)\} \subseteq \mathbb{F}_{q^r}^n.$$

Proposition 1.57. *[9, Theorem 1] The one-point norm-trace code $C(D, mP_\infty)$ is a $[q^{2r-1}, k, d]$ code where the minimum distance d is dependent on the dimension k.*

Specifically,

$$d \geq n - m,$$

$$k = \left| \left\{ x^a y^b : 0 \leq b \leq q^{r-1} - 1, aq^{r-1} + b\left(\frac{q^r - 1}{q - 1}\right) \leq m \right\} \right|$$

Summary

The codes we have covered thus far are Reed-Solomon codes, one-point Hermitian codes, and one-point norm-trace codes. Table 1.1 contains the relevant information for each of these codes, for comparison.

To reiterate, in each of the AG codes defined above, the divisors used are $G = mP_\infty$, and $D = P_1 + \cdots + P_n$ the sum of all other rational points on $\mathcal{X}$ other than P_∞.

Table 1.1: Relevant algebraic geometry codes

Code $C_{\mathcal{L}}(D, G)$	Curve $\mathcal{X}$	Alphabet	Length
Reed-Solomon code	$\mathbb{P}^1_{\mathbb{F}_q}$	$\mathbb{F}_q$	q
Hermitian one-point code	$\mathcal{X}_q : x^{q+1} = y^q + y$	$\mathbb{F}_{q^2}$	q^3
Norm-trace one-point code	$\mathcal{X}_{q,r} : N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x) = \mathrm{Tr}_{\mathbb{F}_q^r/\mathbb{F}_q}(y)$	$\mathbb{F}_{q^r}$	q^{2r-1}

Chapter 2

Norm-trace-lifted codes

Hermitian-lifted codes are defined using Hermitian curves, similar to one-point Hermitian codes, but designed for locality and availability. Hermitian-lifted codes retain the desirable locality of one-point Hermitian codes, while also being advantageous for local recovery with nonzero asymptotic rate. Thus, we consider a more general family of norm-trace curves to use in a similar construction.

The structure of this chapter is as follows. Section 2.1 reviews Hermitian-lifted codes. Section 2.2 discusses the intersection cardinalities of lines with norm-trace curves. Section 2.3 then develops norm-trace-lifted codes. Comparisons to other codes are contained in Section 2.4, detailing rate, parameter, and basis monomial comparisons. Lastly, for norm-trace-lifted codes, a more general result on curve-lifted codes is presented in 2.5, where they are specifically applied to Suzuki curves. Future research directions are contained in Section 2.6, including conjectures related to this work.

2.1 Hermitian-lifted codes

We review the Hermitian-lifted codes of [18] in this section. This material motivates our results in Section 2.3 and provides a natural basis for comparison. Hermitian-lifted codes offer the benefit of having positive rate bounded below by a constant independent of the field size q^2, while retaining the locality afforded by one-point Hermitian codes.

We start with a remark on the number of points of intersection between lines in the projective space $\mathbb{P}^2_{\mathbb{F}_{q^2}}$ and the Hermitian curve $\mathcal{X}_q$.

Remark 2.1. [15] Every non-tangent line over $\mathbb{F}_{q^2}$ intersects the Hermitian curve $\mathcal{X}_q$ over $\mathbb{F}_{q^2}$ in $q+1$ distinct $\mathbb{F}_{q^2}$-rational points.

The Hermitian-lifted codes are defined to capitalize on the property in Remark 2.1. In particular, as we will see, each set of points of intersection between a line and the Hermitian curve forms a repair group of size $q+1$. On each line, only functions which restrict to low-degree univariate polynomials are evaluated to define codewords. The functions restricted to these lines give univariate polynomials. Then local recovery can take place by accessing only those q coordinates corresponding to points on the line, rather than all other q^2-1 points.

Thus, Remark 2.1 affects the desired degree of the polynomials to which functions $f(x,y) \in \mathbb{F}_q[x,y]$ restrict, motivating Definition 2.2.

Definition 2.2. Let

$$\mathbb{L} \coloneqq \{L_{\alpha,\beta}(t) : \alpha \in \mathbb{F}_{q^2} \backslash \{0\}, \beta \in \mathbb{F}_{q^2}\}$$

be the set of lines of the form

$$L_{\alpha,\beta}(t) = (t, \alpha t + \beta).$$

Given $f \in \mathbb{F}_{q^2}[x,y]$, $g \in \mathbb{F}_{q^2}[t]$, and $L_{\alpha,\beta} : \mathbb{F}_{q^2}[t] \to \mathbb{F}_{q^2}^2$, we say that $f \circ L_{\alpha,\beta}$ *agrees with* g *on* $\mathcal{X}_q$, and write

$$f \circ L_{\alpha,\beta} \equiv_{\mathcal{X}_q} g,$$

if

$$f(L_{\alpha,\beta}(t)) = g(t)$$

for all $t \in \mathbb{F}_{q^2}$ with $L_{\alpha,\beta}(t) \in \mathcal{X}_q$.

Let

$$\mathcal{F} \coloneqq \left\{ f \in \mathbb{F}_{q^2}[x,y] : \begin{array}{l} \forall L_{\alpha,\beta} \in \mathbb{L}, \exists g \in \mathbb{F}_{q^2}[t]_{<q} \\ \text{and } f \circ L_{\alpha,\beta} \equiv_{\mathcal{X}_q} g \end{array} \right\}.$$

Definition 2.3. Let $n = q^3$, and $\mathcal{X}(\mathbb{F}_{q^2}) \coloneqq \{P_1, \ldots, P_n\}$. The *Hermitian-lifted code* on $\mathbb{F}_{q^2}$ is

$$\mathcal{C}_{\mathcal{X}_q} \coloneqq \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{F}\} \subseteq \mathbb{F}_{q^2}^n.$$

The Hermitian-lifted code is designed so that if any coordinate $c_i = f(P_i)$ for $i \in [n]$ is erased, then c_i can be recovered from the other coordinates corresponding to any line on which the evaluation point P_i lies. Then, Reed-Solomon interpolation may be utilized in order to recover the coordinate.

It is relevant to consider the composition $M_{a,b} \circ L_{\alpha,\beta}(t)$ of a monomial $M_{a,b}(x,y) = x^a y^b$ with a line $L_{\alpha,\beta}$ modulo a polynomial of interest resulting from the curve. It is this condition that allows recovery of erasures which occur in a given repair group. That is because the repair groups are formed by intersections of lines in $\mathbb{F}_{q^2}^2$ with the Hermitian curve. The definitions given below build towards the definition of a good monomial.

Definition 2.4. Given $\alpha, \beta \in \mathbb{F}_{q^2}$, define

$$p_{\alpha,\beta}(t) \coloneqq t^{q+1} + \alpha^q t^q + \alpha t + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta) \in \mathbb{F}_{q^2}[t].$$

For a polynomial $g(t) \in \mathbb{F}_{q^2}[t]$, define $\hat{g}_{\alpha,\beta}(t)$ to be the remainder resulting from dividing $g(t)$ by $p_{\alpha,\beta}(t)$; i.e.

$$\hat{g}_{\alpha,\beta}(t) \coloneqq g(t) \bmod p_{\alpha,\beta}(t).$$

Set

$$\deg_{\alpha,\beta}(g) \coloneqq \deg(\hat{g}_{\alpha,\beta}(t)).$$

Notice that $\deg_{\alpha,\beta}(g) \leq q$ for all $g \in \mathbb{F}_{q^2}[t]$, as $\deg(p_{\alpha,\beta}(t) = q+1$.

Based on Remark 2.1, we are interested in monomials $f(x,y)$ such that

$$\deg_{\alpha,\beta}(f \circ L_{\alpha,\beta}) < q.$$

Definition 2.5. A monomial $M_{a,b}(x,y) = x^a y^b$ is said to be *good* for $\mathcal{X}_q$ if for all lines $L_{\alpha,\beta} \in \mathbb{L}$,

$$\deg_{\alpha,\beta}(M_{a,b} \circ L_{\alpha,\beta}) < q.$$

Remark 2.6. As opposed to one-point Hermitian codes, Hermitian-lifted codes have a rate bounded below by a constant independent of the field size [18]. Specifically, it is shown that the rate is bounded below by 0.007. This rate results from showing that there are sufficiently many good monomials yielding linearly independent codewords. The actual number of good monomials remains an open question.

We consider only one-point Hermitian codes with evaluation functions $\mathcal{L}(mP_\infty)$ where $m \leq q^2-1$. For monomials $x^a y^b \in \mathcal{L}((q^2-1)P_\infty)$, the degree of the monomial restricted to a line is $a+b$, since

$$(M_{a,b} \circ L_{\alpha,\beta})(t) = (t)^a(\alpha t + \beta)^b.$$

For $M_{a,b} \circ L_{\alpha,\beta} \in \mathcal{F}$, $a+b \leq q-1$. Recall that $aq + b(q+1) \leq q^2-1$ for $x^A y^b \in \mathcal{L}(mP_\infty)$, which in turn gives

$$a+b \leq \left\lfloor \frac{q^2-1-b}{q} \right\rfloor = q-1.$$

Thus, if $m \leq q^2-1$, we then have natural locality for the one-point Hermitian codes.

However, with this restriction, the rate of the one-point Hermitian code $C_{\mathcal{L}}(D, mP_\infty)$ is no more than

$$\frac{m+1}{q^3} \leq \frac{1}{q} \to 0 \text{ as } q \to \infty,$$

as mentioned in [18, Observation 2].

While it is true that rate for Hermitian-lifted codes $\mathcal{C}_{\mathcal{X}_q}$ are better than one-point Hermitian codes $C_{\mathcal{L}}(D, mP_\infty)$, Hermitian-lifted codes suffer from a lack of expression for the evaluation polynomials. The monomials $x^a y^b$ which form a basis for $\mathcal{L}(mP_\infty)$ are exactly those which satisfy $aq+b(q+1) \leq m$. In contrast, no expression has yet been formulated for the monomials which form a basis for $\mathcal{F}$, which consists of the monomials in $\mathcal{L}(mP_\infty)$ in addition to a new set of monomials.

2.2 Intersection numbers

For Hermitian-lifted codes, the locality (and thus the upper bound on the degree of the polynomials g that the functions $f \in \mathcal{F}$ needed to satisfy when restricted) comes from Remark 2.1, a result on the intersection of lines with Hermitian curves. It is convenient that this result for the Hermitian curve exists, since it is crucial to the defining of Hermitian-lifted codes. We will use intersection numbers to adapting the Hermitian-lifted code construction to other families of curves. A precise definition is given next.

Definition 2.7. Let $\mathcal{X}$ be an algebraic curve on $\mathbb{F}_q^2$, and $L_{\alpha,\beta}$ be a line over $\mathbb{F}_q$. The *intersection number* between the curve $\mathcal{X}$ and the line $L_{\alpha,\beta}$ is the number of distinct affine points of intersection in $\mathbb{F}_q^2$.

The intersection number is the number of points for which we consider Reed-Solomon-like erasure recovery. The point at infinity is not included, because the evaluation functions for

the codes considered in this work have poles there. Multiplicities at affine points P are irrelevant, because only one evaluation can be used.

To define norm-trace-lifted codes, we need a result similar to Remark 2.1 on the intersection between lines and the curves $\mathcal{X}_{q,r}$. Such a result on the intersection number $|L_{\alpha,\beta} \cap \mathcal{X}_{q,r}|$ defines how high the degree a polynomial g can restrict to when considered over the intersection $L_{\alpha,\beta} \cap \mathcal{X}_{q,r}$. Therefore, it is necessary to have the intersection numbers $|L_{\alpha,\beta} \cap \mathcal{X}_{q,r}|$ with non-tangent lines to define norm-trace-lifted codes.

Note the benefit of $|L_{\alpha,\beta} \cap \mathcal{X}_q| = q + 1$ for the Hermitian curve. Because of this result, all non-tangent lines serve as repair groups. Lemma 2.10 in Section 2.2 accomplishes the same goal; because we will determine

$$|L_{\alpha,\beta} \cap \mathcal{X}_{2,r}| \in \{2^{r-1} - 1, 2^{r-1} + 1\}$$

for non-tangent lines. Thus, all non-tangent lines continue to form repair groups of size $2^{r-1} - 1$. Computation suggests that norm-trace curves have a similar property, as seen in Section 2.2, though this property has not been proven for all norm-trace curves.

In general, the intersection number $|L_{\alpha,\beta} \cap \mathcal{X}|$ between an arbitrary algebraic curve $\mathcal{X}$ and line $L_{\alpha,\beta}$ is not known. Upper bounds do not suffice for our purpose, because the points are needed for interpolation. For this reason, we restrict our attention to the case when $q = 2$, where we can determine cardinalities of the intersections between lines and norm-trace curves.

Norm-trace curves

We do not consider horizontal lines because many of these lines are tangent, and so the intersection between horizontal lines and the curve is not conducive for forming repair groups. In particular, it may only contain a single point. We give a proof of this result below.

Definition 2.8. Let

$$\mathbb{L} \coloneqq \{L_{\alpha,\beta}(t) : \alpha \in \mathbb{F}_{2^r} \backslash \{0\}, \beta \in \mathbb{F}_{2^r}\}$$

be the set of lines of the form

$$L_{\alpha,\beta}(t) = (t, \alpha t + \beta).$$

In this work we denote the set of points on a line as

$$L_{\alpha,\beta} = \{L_{\alpha,\beta}(t) : t \in \mathbb{F}_{2^r}\}.$$

Lemma 2.9. *Let $q = 2$, and consider the norm-trace curve $\mathcal{X}_{2,r}$ over $\mathbb{F}_{2^r}$ with $r \geq 2$. The intersection between a line $L_{0,\beta} \equiv \beta \in \mathbb{L}$ and $\mathcal{X}_{2,r}$ over $\mathbb{F}_{2^r}$ has cardinality of 1 or $2^r + 1$, meaning $|L_{0,\beta} \cap \mathcal{X}_{2,r}| \in \{1, 2^r + 1\}$.*

Proof. The curve $\mathcal{X}_{2,r}$ we consider is written as

$$x^{2^r-1} = y^{2^{r-1}} + \cdots + y^2 + y,$$

and we represent lines $L_{\alpha,\beta}(t)$ as pairs $(t, \alpha t + \beta) \in \mathbb{F}_{2^r}^2$. Then, points in the intersection $L_{\alpha,\beta} \cap \mathcal{X}_{2,r}$ correspond to values t that satisfy the equation

$$t^{2^r-1} = \beta^{2^{r-1}} + \cdots + \beta^2 + \beta = \mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta).$$

The number of $t \in \mathbb{F}_{2^r}$ which are the roots of the polynomial $h(t) = t^{2^r-1} + \mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta)$ is exactly the cardinality of the intersection $L_{\alpha,\beta} \cap \mathcal{X}_{2,r}$.

To find the number of such $t \in \mathbb{F}_{2^r}$, we wish to find the degree of $d(t) = \gcd(h(t), t^{2^r} - t)$, with two cases of β, which can only be 0 or 1. The reason finding this degree suffices is that $t^{2^r} - t$ has as its roots all 2^r elements of $\mathbb{F}_{2^r}$ as simple zeros.

Case 1: Let $\mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta) = 0$. We use the Euclidean algorithm to find the gcd, writing each step in the form $a = qb + r$:

$$t^{2^r} - t = (t^{2^r-1}) \cdot (t) + t$$

$$t^{2^r-1} = (t) \cdot (t^{2^r-2}) + (0)$$

Then

$$\gcd(h(t), t^{2^r} - t) = t$$

since the degree of this polynomial is 1, $|L_{\alpha,\beta} \cap \mathcal{X}_{2,r}| = 1$.

Case 2: Let $\mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta) = 1$. We again use the Euclidean algorithm, writing each step in the form $a = qb + r$:

$$t^{2^r} - t = (t^{2^r-1} + 1) \cdot (t) + (0)$$

Then

$$\gcd(h(t), t^{2^r} - t) = t^{2^r-1} + 1$$

since the degree of this polynomial is $2^r - 1$, $|L_{\alpha,\beta} \cap \mathcal{X}_{2,r}| = 2^r + 1$. ■

Now we discuss non-horizontal lines. The following result captures the necessary information to describe the locality of the code to be constructed.

Lemma 2.10. *Let $q = 2$, and consider the norm-trace curve over $\mathbb{F}_{2^r}$ with $r \geq 2$. The intersection between a line $L_{\alpha,\beta} \in \mathbb{L}$ with $\alpha \neq 0$ and the norm-trace curve $\mathcal{X}_{2,r}$ over $\mathbb{F}_{2^r}$ has*

cardinality $2^{r-1}-1$ *or* $2^{r-1}+1$*, that is,*

$$|\mathcal{X}_{2,r} \cap L_{\alpha,\beta}| \in \{2^{r-1}-1, 2^{r-1}+1\}.$$

Proof. The curve $\mathcal{X}_{2,r}$ we consider is written as

$$x^{2^r-1} = y^{2^{r-1}} + \cdots + y^2 + y$$

and we represent lines $L_{\alpha,\beta}(t)$ as pairs $(t, \alpha t+\beta) \in \mathbb{F}_{2^r}^2$. Points in the intersection $L_{\alpha,\beta} \cap \mathcal{X}_{2,r}$ correspond to values t that satisfy the equation

$$t^{2^r-1} = (\alpha t+\beta)^{2^{r-1}} + \cdots + (\alpha t+\beta)^2 + (\alpha t+\beta).$$

Expanding the terms on the right with the Freshman's Dream, we get

$$t^{2^r-1} = (\alpha t)^{2^{r-1}} + \beta^{2^{r-1}} + \cdots + (\alpha t)^2 + \beta^2 + \alpha t + \beta$$

$$t^{2^r-1} = \alpha^{2^{r-1}} t^{2^{r-1}} + \cdots + \alpha^2 t^2 + \alpha t + \mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta)$$

$$h(t) \coloneqq t^{2^r-1} + \alpha^{2^{r-1}} t^{2^{r-1}} + \cdots + \alpha^2 t^2 + \alpha t + \mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta) = 0$$

The number of $t \in \mathbb{F}_{2^r}$ which satisfy $h(t)$ is exactly the cardinality of the intersection $L_{\alpha,\beta} \cap \mathcal{X}_{2,r}$.

To find the number of such $t \in \mathbb{F}_{2^r}$, we wish to find the degree of $d(t) = \gcd(h(t), t^{2^r} - t)$. Since $t^{2^r} - t$ factors into distinct linear terms over $\mathbb{F}_{2^r}$, so does $d(t)$. Thus, the number of points of intersection is exactly the degree of $d(t)$. The reason finding this degree suffices is that $t^{2^r} - t$ has as its roots all 2^r elements of $\mathbb{F}_{2^r}$ as simple zeros. Because the field trace of β can only be 0 or 1, we consider two cases as follows.

Case 1: Let $\mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta) = 0$. We use the Euclidean algorithm to find the gcd, writing each step in the form $a = qb + r$. This work is expanded on following this lemma.

$$t^{2^r} - t = (t^{2^r-1} + \alpha^{2^{r-1}} t^{2^{r-1}} + \cdots + \alpha^2 t^2 + \alpha t) \cdot (t) + (\alpha^{2^{r-1}} t^{2^{r-1}+1} + \cdots + \alpha t^2 + t)$$

$$t^{2^r-1} + \alpha^{2^{r-1}} t^{2^{r-1}} + \cdots + \alpha^2 t^2 + \alpha t = (\alpha^{2^{r-1}} t^{2^{r-1}+1} + \cdots + \alpha t^2 + t) \cdot (\alpha^{2^{r-1}-1} t^{2^{r-1}-2} + \cdots + \alpha^3 t^2 + \alpha) + (0)$$

To demonstrate the product above, see terms of these polynomials multiplied in Table 2.1. Since the desired polynomial for this product is $t^{2^r-1} + (\alpha t)^{2^{r-1}} + \cdots + (\alpha t)^2 + \alpha t$, those entries are boxed in Table 2.1. Notice that these are the only entries that do not appear twice in the table (and thus will not be canceled out when all the terms are added up).

Then

$$\gcd(h(t), t^{2^r} - t) = \alpha^{2^{r-1}} t^{2^{r-1}+1} + \cdots + \alpha t^2 + t$$

since the degree of this polynomial is $2^{r-1} + 1$, $|L_{\alpha,\beta} \cap \mathcal{X}_{2,r}| = 2^{r-1} + 1$.

Case 2: Let $\mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta) = 1$. We again use the Euclidean algorithm, writing each step in the form $a = qb + r$:

$$t^{2^r} - t = (t^{2^r-1} + \alpha^{2^{r-1}} t^{2^{r-1}} + \cdots + \alpha^2 t^2 + \alpha t + 1) \cdot (t) + (\alpha^{2^{r-1}} t^{2^{r-1}+1} + \cdots + \alpha t^2)$$

$$t^{2^r-1} + \alpha^{2^{r-1}} t^{2^{r-1}} + \cdots + \alpha t + 1 = (\alpha^{2^{r-1}} t^{2^{r-1}+1} + \cdots + \alpha t^2) \cdot (\alpha^{2^{r-1}-1} t^{2^{r-1}-2} + \cdots + \alpha) + (\alpha^{2^{r-1}-1} t^{2^{r-1}-1} + \cdots + 1)$$

$$\alpha^{2^{r-1}-1} t^{2^{r-1}+1} + \cdots + \alpha t^2 = (\alpha^{2^{r-1}} t^{2^{r-1}-1} + \cdots + \alpha) \cdot (\alpha t^2) + (0)$$

Table 2.1 contains all the details to justify this factorization. The product in the expression above consists of all the entries except those in the last column. Notice that these are exactly the terms in the remainder proposed above, with the exception of missing terms $\alpha t + 1$.

Then

$$\gcd(h(t), t^{2^r} - t) = \alpha^{2^{r-1}} t^{2^{r-1}-1} + \cdots + \alpha$$

since the degree of this polynomial is $2^{r-1} - 1$, $|L_{\alpha,\beta} \cap \mathcal{X}_{2,r}| = 2^{r-1} - 1$. ■

Table 2.1: Lemma 2.10 multiplication table

	$\alpha^{2^{r-1}} t^{2^{r-1}+1}$	$\alpha^{2^{r-2}} t^{2^{r-2}+1}$	$\cdots$	$\alpha^2 t^3$	αt^2	t
$\alpha^{2^{r-1}-1} t^{2^{r-1}-2}$	$\boxed{t^{2^r-1}}$	$(\alpha t)^{2^{r-1}+2^{r-2}+\cdots+1}$		$(\alpha t)^{2^{r-1}+1}$	$\boxed{(\alpha t)^{2^{r-1}}}$	$(\alpha t)^{2^{r-1}-1}$
$\alpha^{2^{r-1}-1} t^{2^{r-1}-2}$	$(\alpha t)^{2^{r-1}+2^{r-2}-1}$	$(\alpha t)^{2^{r-1}-1}$	$\cdots$	$(\alpha t)^{2^{r-2}+1}$	$\boxed{(\alpha t)^{2^{r-2}}}$	$(\alpha t)^{2^{r-2}-1}$
$\alpha^{2^{r-1}-1} t^{2^{r-1}-2}$	$(\alpha t)^{2^{r-1}+2^{r-3}-1}$	$(\alpha t)^{2^{r-2}+2^{r-3}+\cdots+1}$		$(\alpha t)^{2^{r-3}+1}$	$\boxed{(\alpha t)^{2^{r-3}}}$	$(\alpha t)^{2^{r-3}-1}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$\alpha^{15} t^{14}$	$(\alpha t)^{2^{r-1}+15}$	$(\alpha t)^{2^{r-2}+15}$	$\cdots$	$(\alpha t)^{17}$	$\boxed{(\alpha t)^{16}}$	$(\alpha t)^{15}$
$\alpha^7 t^6$	$(\alpha t)^{2^{r-1}+7}$	$(\alpha t)^{2^{r-2}+7}$	$\cdots$	$(\alpha t)^9$	$\boxed{(\alpha t)^8}$	$(\alpha t)^7$
$\alpha^3 t^2$	$(\alpha t)^{2^{r-1}+3}$	$(\alpha t)^{2^{r-2}+3}$	$\cdots$	$(\alpha t)^5$	$\boxed{(\alpha t)^4}$	$(\alpha t)^3$
α	$(\alpha t)^{2^{r-1}+1}$	$(\alpha t)^{2^{r-2}+1}$	$\cdots$	$(\alpha t)^3$	$\boxed{(\alpha t)^2}$	$\boxed{(\alpha t)^1}$

Norm-trace curves, computational results

Lemma 2.10 gives the exact intersection numbers of norm-trace curves with non-horizontal lines for the case when $q = 2$. We already have the exact intersection number when $r = 2$

from Remark 2.1. An open question is what intersection numbers between non-horizontal lines and norm-trace curves are in general.

Table 2.2 gives computational results for these intersection numbers, where q is along the top of the chart, and r is along the left-hand side, and any entry with a star ($*$) is one where only a subset of the line intersection numbers were computed (and so there may still be more possible intersection numbers in those cases). Keep in mind again that these are the intersections with non-horizontal lines shown in these tables.

Table 2.2: Intersection numbers of lines with norm-trace curves

	$q=3$	$q=4$	$q=5$	$q=7$	$q=8$	$q=9$
$r=3$	7,10	13,17,21	21,26,31	43,50,57$*$	57,65,73$*$	73,82,91$*$
$r=4$	22,28,31	49,69	111,121,126,141$*$	351,377$*$	489,505,513,537$*$	
$r=5$	76,91	245,257,277$*$	621,626$*$			
$r=6$	229,244,256$*$	981,1025,1045$*$				
$r=7$	742,793$*$					

For $q \geq 9$, we were only able to get partial computational results when $r = 3$; we present those results in Table 2.3.

Table 2.3: Intersection numbers of lines with norm-trace curves with $r = 3$

	$q=11$	$q=13$	$q=16$	$q=17$
$r=3$	111,122,133$*$	157,170,183$*$	241,257,273$*$	273,290,307$*$

Note that there seem to be only a few closely-clustered values for intersection numbers of the norm-trace curves with non-horizontal lines. This pattern is also true of the partially computed examples. There seem to be only a few possible values for intersection numbers, that is, out of all q^r possible points which a line occupies in $\mathbb{F}_{q^r}^2$, only a couple possible numbers for intersection cardinalities seem to exist. If this property were proven to hold for all norm-trace curves, then additional norm-trace curves would be a good candidate to replace the Hermitian curve in the Hermitian-lifted code construction.

Quotients of norm-trace curves, computational results

This project was inspired by the fact that norm-trace curves are a natural generalization of Hermitian curves. However, the Hermitian curves are special among norm-trace curves in the sense that they are maximal. With this property of the Hermitian curve considered, one may want to consider other maximal curves (particularly curves covered by the Hermitian curve) in this code-lifting construction [8]. We give the defining equations for these curves below.

Consider a quotient of the Hermitian function field over $\mathbb{F}_{q^2}$ has defining equation

$$x^u = y^q + y$$

where $u|(q+1)$, and consider a quotient of a norm-trace function field over $\mathbb{F}_{q^2}$ has defining equation

$$x^u = y^{q^{r-1}} + \cdots + y$$

where $u|\frac{q^r-1}{q-1}$.

However, the computational evidence suggests these curves may not be good candidates since the intersection cardinalities between lines and these curves is quite varied. This observation is in contrast to the norm-trace curves over binary fields, which had only a few possibilities for intersection numbers, and in general the lines exhibited a relatively uniform distribution among the few intersection numbers. A computational example which shows the quotients do not in general demonstrate clustering behavior is given in Figure 2.1.

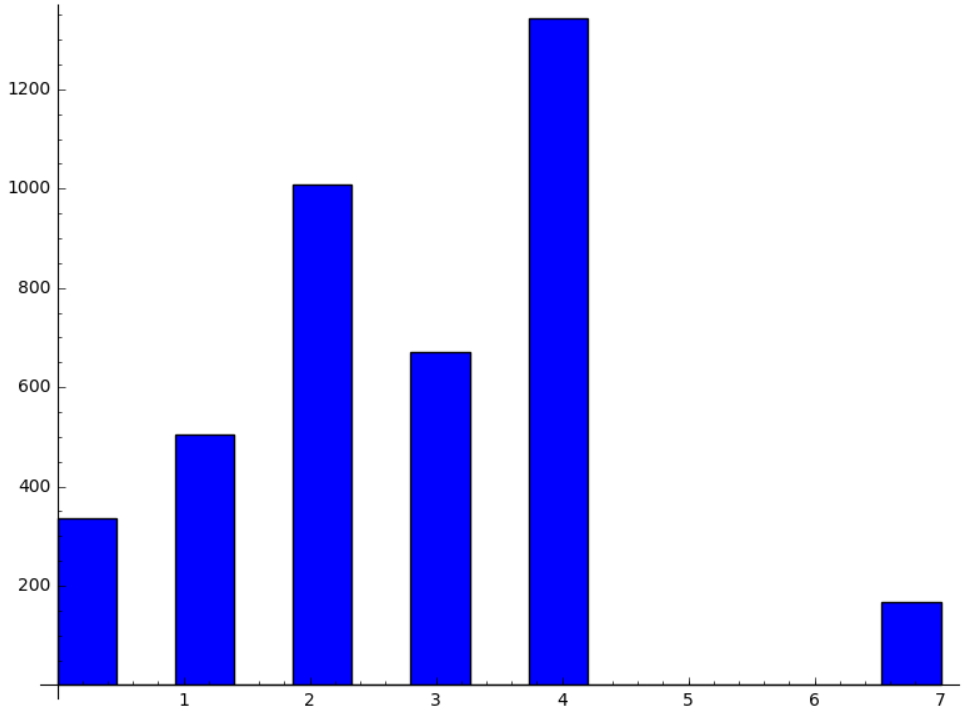

Figure 2.1: Distribution of intersection numbers of lines with $x^3 = y^8 + y$ (over $\mathbb{F}_{64}$).

2.3 Norm-trace-lifted codes

Given Lemma 2.10, we now have the information on locality necessary to define norm-trace-lifted codes. Recall that for the affine curve $\mathcal{X}_{2,r}$ over $\mathbb{F}_{q^r}$, $|\mathcal{X}_{2,r}| = 2^{2r-1}$. While there is strong inspiration from Hermitian-lifted codes, we will see that some key differences make the norm-trace-lifted codes attractive.

Definition 2.11. For $f \in \mathbb{F}_{2^r}[x, y]$ and $g \in \mathbb{F}_{2^r}[t]$ and a line $L_{\alpha,\beta} : \mathbb{F}_{2^r} \to \mathbb{F}_{2^r}^2$, we say that $f \circ L_{\alpha,\beta}$ *agrees with* g *on* $\mathcal{X}_{2,r}$, and write

$$f \circ L_{\alpha,\beta} \equiv_{\mathcal{X}_{2,r}} g,$$

if $f(L_{\alpha,\beta}(t)) = g(t)$ for all $t \in \mathbb{F}_{2^r}$ with $L_{\alpha,\beta}(t) \in \mathcal{X}_{2,r}$.

Definition 2.12. Let $\mathcal{F}$ be given by

$$\mathcal{F} \coloneqq \left\{ f \in \mathbb{F}_{2^r}[x,y] : \begin{array}{l} \forall L_{\alpha,\beta} \in \mathbb{L}, \exists g \in \mathbb{F}_{2^r}[t]_{<2^{r-1}-2} \\ \text{and } f \circ L_{\alpha,\beta} \equiv_{\mathcal{X}_{2,r}} g \end{array} \right\}.$$

We define $\mathbb{L}$ this way because horizontal lines, lines with $\alpha = 0$, intersect the curve $\mathcal{X}_{2,r}$ in either 1 or $2^r - 1$ affine points, as shown in Section 2.2. This exclusion of lines affects the availability of Theorem 2.18, but only slightly, because each point has only one horizontal line which passes through it.

Definition 2.13. The *norm-trace-lifted code* $\mathcal{C} \subseteq (\mathbb{F}_{2^r})^{2^{2r-1}}$ is the evaluation code

$$\mathcal{C}_{\mathcal{X}_{2,r}} \coloneqq \{(f(x,y))_{(x,y)\in\mathcal{X}_{2,r}(\mathbb{F}_{2^r})} : f \in \mathcal{F}\}.$$

Next, we consider the parameters of $\mathcal{C}_{\mathcal{X}_{2,r}}$. We show the rate of the norm-trace-lifted codes with $q = 2$ is asymptotically a nonzero constant with larger lower bound for large q than Hermitian-lifted codes. First, we review the Hermitian-lifted code analog.

Recall that a good monomial is a monomial which restricts to a sufficiently low-degree polynomial on the intersection of a line with the relevant curve; in the case of Hermitian-lifted codes, the Hermitian curve $\mathcal{X}_q$ is the relevant curve. This requirement that the restriction be low-degree is in order to allow for recovery of information by accessing only information from the points in the intersection. There are two types of good monomials $x^a y^b \in \mathcal{F}$ for Hermitian-lifted codes: those with $a + b < q$, and those with $a + b \geq q$. Explicit expressions are not known in the case $a + b \geq q$.

This distinction is important because the basis for the evaluation functions of one-point Hermitian codes consist only of monomials where $a + b < q$, while the Hermitian-lifted codes

basis contains those monomials as well as a set of good monomials with $a + b \geq q$. It is those good monomials with $a + b \geq q$ which cause the Hermitian-lifted codes to have an asymptotically nonzero rate, while in contrast the asymptotic rate of one-point Hermitian codes is zero.

For Hermitian-lifted codes, it is the case that when $a + b < q$ for a monomial $x^a y^b$, that the $x^a y^b \in \mathcal{F}$. If $a + b < q$, then $M_{a,b} \circ L_{\alpha,\beta}$ has degree in its remainder less than q for all lines $L_{\alpha,\beta}$ regardless of any division done to it by the polynomial

$$p(t) = t^{q+1} + (\alpha t)^q + \alpha t + \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta).$$

However, the number of such monomials is $\frac{q(q+1)}{2}$ by counting, and the rate

$$\frac{\binom{q(q+1)}{2}}{q^3} = \frac{1}{2q} + \frac{1}{2q^2} \to 0 \text{ as } q \to \infty.$$

Hence, the monomials with $a + b > q$ needed to be counted in [18] to guarantee that the rate is asymptotically bounded away from zero. It was identified as an open and challenging problem to describe such monomials.

However, as we will see, the situation is different for norm-trace-lifted codes; that is, counting the monomials $x^a y^b$ which have $a + b$ less than the locality of $2^{r-1} - 2$ is enough to give an asymptotically nonzero rate. The following results state this fact more succinctly.

Lemma 2.14. *Let $M_{a,b} = x^a y^b$. Then the set of vectors*

$$\left\{(M_{a,b}(x,y))_{(x,y)\in\mathcal{X}_{q,r}} : 0 \leq a \leq q^{r-1} - 1, 0 \leq b \leq q^r - 1\right\}$$

are linearly independent.

Proof. We draw inspiration from [18]. The kernel of the evaluation map

$$\begin{aligned} ev: \quad \mathcal{L}(mP_\infty) &\to \mathbb{F}_{q^r}^n \\ f &\mapsto (f(P_1), \ldots, f(P_{q^r})). \end{aligned}$$

of the q^r affine points of the norm-trace curve $\mathcal{X}_{q,r}$ is generated by

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

$$x^{q^r} - x,$$

and

$$y^{q^r} - y.$$

Under monomial orderings with $x^{\frac{q^r-1}{q-1}} < y^{q^{r-1}}$, $\left\{x^{\frac{q^r-1}{q-1}} - y^{q^{r-1}} - \cdots - y^q - y, x^{q^r} - x\right\}$ is a Gröbner basis for the kernel of the evaluation map, and so the evaluations of $M_{a,b}$ cannot contain any element from the kernel of the evaluation map. Thus, the evaluations of $M_{a,b}$ are linearly independent. ■

Thus, if we count the number of such good monomials with $a + b < 2^{r-1} - 2$, we will get a lower bound on dimension, and thus a lower bound on the rate.

As in [18, Definition 5], it is relevant to consider the composition $M_{a,b} \circ L_{\alpha,\beta}(t)$ modulo a polynomial of interest resulting from the curve; the precise definitions are given below.

Definition 2.15. Given $\alpha, \beta \in \mathbb{F}_{2^r}$, define

$$p_{\alpha,\beta}(t) := t^{2^{r-1}} + \alpha^{2^{r-1}} t^{2^{r-1}} + \cdots + \alpha t + \mathrm{Tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(\beta) \in \mathbb{F}_{q^r}[t].$$

For a polynomial $g(t) \in \mathbb{F}_{2^r}[t]$, define $\hat{g}_{\alpha,\beta}(t)$ to be the remainder resulting from dividing $g(t)$

by $p_{\alpha,\beta}(t)$, i.e.

$$\hat{g}_{\alpha,\beta}(t) \coloneqq g(t) \bmod p_{\alpha,\beta}(t).$$

Set

$$\deg_{\alpha,\beta}(g) \coloneqq \deg(\hat{g}_{\alpha,\beta}(t)).$$

Notice that $\deg_{\alpha,\beta}(g) \leq 2^{r-1} - 2$ for all $g \in \mathbb{F}_{2^r}[t]$, as $\deg(p_{\alpha,\beta}(t)) = 2^{r-1} - 1$.

With the above definition, we note that we are interested in monomials $M_{a,b}(x, y)$ such that

$$\deg_{\alpha,\beta}(M_{a,b} \circ L_{\alpha,\beta}) < 2^{r-1} - 2.$$

Definition 2.16. A monomial $M_{a,b}(x, y)$ is said to be *good* for $\mathcal{X}_{2,r}$ if for all lines $L_{\alpha,\beta} \in \mathbb{L}$,

$$\deg_{\alpha,\beta}(M_{a,b} \circ L_{\alpha,\beta}) < 2^{r-1} - 2.$$

Note that if $M_{a,b}$ is good, then $M_{a,b} \in \mathcal{F}$. We wish to find a large set of good monomials due to Lemma 2.14.

Lemma 2.17. *Consider the norm-trace curve over $\mathbb{F}_{2^r}$ with $r \geq 2$. The rate of the norm-trace-lifted code over $\mathbb{F}_{2^r}$ is asymptotically 0.25. For each r, there is some number ε_r where the rate of the code over $\mathbb{F}_{2^r}$ is $0.25 - \varepsilon_r$, where $\varepsilon_r \to 0$ as $r \to \infty$.*

Proof. First observe that if $M_{a,b}$ is good, $M_{a,b} \in \mathcal{F}$. Since the locality of the code is $2^{r-1} - 2$ by Lemma 2.10, we now count the monomials $x^a y^b$ which have $a + b < 2^{r-1} - 2$. The number of such monomials is

$$\frac{(2^{r-1} - 2)(2^{r-1} - 1)}{2} = \frac{2^{2r-2} - 2^r - 2^{r-1} + 2}{2} = 2^{2r-3} - 2^{r-1} - 2^{r-2} + 1.$$

Then, since the number of affine points on $\mathcal{X}_{2,r}$ is 2^{2r-1}, the rate of the norm-trace-lifted code is

$$\frac{2^{2r-3} - 2^{r-1} - 2^{r-2} + 1}{2^{2r-1}} = \frac{1}{4} - \frac{1}{2^r} - \frac{1}{2^{r+1}} + \frac{1}{2^{2r-1}}.$$

Since

$$\frac{1}{4} - \frac{1}{2^r} - \frac{1}{2^{r+1}} + \frac{1}{2^{2r-1}} \to \frac{1}{4} \text{ as } r \to \infty.$$

The rate is asymptotically bounded below by $\frac{1}{4} = 0.25$.

However, we may also show that there are no such good monomials $x^a y^b$ with $a+b \geq 2^{r-1}-2$. Recall that $0 \leq a \leq 2^r$ and $0 \leq b \leq 2^{r-1}$, and again that the locality of the code is $2^{r-1} - 2$. To show that a monomial $M_{a,b}$ is not good, we must find some line L_{α^*,β^*} such that $\deg_{\alpha^*,\beta^*}(M_{a,b} \circ L_{\alpha^*,\beta^*}) \geq 2^{r-1} - 2$.

We consider the following cases to show that no monomials with $a + b \geq 2^{r-1} - 2$ are good. In each case consider the specific line $L_{1,0}(t) = (t, t)$, in other words we consider $(M_{a,b} \circ L_{1,0})(t) = t^{a+b}$.

Case 1: Let $2^{r-1} - 2 < a + b < 2^r - 1$. Because the degree of $p_{1,0}(t)$ is $2^r - 1$,

$$\deg_{\alpha,\beta}(M_{a,b} \circ L_{1,0}) = \deg_{\alpha,\beta}(t^{a+b}) = a + b > 2^{r-1} - 2.$$

Thus, the monomial $M_{a,b}$ is not good.

Case 2: Let $a + b = 2^r - 1$. Then,

$$\deg_{\alpha,\beta}(M_{a,b} \circ L_{1,0}) = \deg_{\alpha,\beta}(t^{a+b}) = 2^{r-1} > 2^{r-1} - 2,$$

since $t^{2^{r-1}} = t^{2^{r-1}} + \cdots + t$. Again the monomial $M_{a,b}$ is not good.

Case 3: Let $2^r - 1 < a + b \leq 2^r + 2^{r-1}$. Then, extending on the previous case,

$$\deg_{\alpha,\beta}(M_{a,b} \circ L_{1,0}) = \deg_{\alpha,\beta}(t^{a+b}) > 2^{r-1} > 2^{r-1} - 2.$$

Hence, the monomial $M_{a,b}$ is not good.

Since in each of the cases above, $\deg_{\alpha,\beta}(M_{a,b} \circ L_{1,0}) > 2^{r-1} - 2$, there are no good monomials with $a + b \geq 2^{r-1} - 2$. Therefore the rate of the code is exactly $0.25 - \varepsilon_r$. ■

In this section we showed the rate of the norm-trace-lifted codes is asymptotically a nonzero constant. The norm-trace curve also provides the following benefits over the Hermitian curve in this construction:

- The rates of norm-trace-lifted codes asymptotically are better than those of the Hermitian-lifted codes. Clearly $0.25 > 0.007$, and beyond this observation, the highest rate given in the computational examples of [18] is 0.20, and the Hermitian-lifted code rates only decrease as $q \to \infty$.
- The good monomials $x^a y^b$ used in the norm-trace-lifted codes are easier to identify, because the only requirement we have is that $a + b < 2^{r-1} - 2$. This benefit is in contrast to the Hermitian-lifted codes, where classifying the good monomials remains a difficult problem.

Together with the results above from Section 2.2, we may now completely describe the parameters of norm-trace-lifted codes. The following theorem summarizes the work done thus far to determine the parameters of norm-trace-lifted codes.

Theorem 2.18. *Let $\mathcal{C}$ be the norm-trace-lifted code arising from $\mathcal{X}_{2,r}$. Then the code $\mathcal{C}$ is an $[2^{2r-1}, (0.25 - \varepsilon_r) \cdot 2^{2r-1}, \geq 2^r]$ code, with locality $2^{r-1} - 2$ and availability $2^r - 1$.*

Proof. First, we note that the results from Lemma 2.10 directly give the locality. Since each line in $\mathbb{L}$ intersects the curve $\mathcal{X}_{2,r}$ in exactly $2^{r-1}-1$ or $2^{r-1}+1$ distinct affine points, the locality is $(2^{r-1}-1)-1 = 2^{r-1}-2$. The dimension follows from Lemma 2.17.

Next we determine availability, which is the number of lines that pass through a given point which intersect the curve in at least $2^{r-1}-1$ points. As this result describes all non-tangent lines in the space, we count the number of non-tangent lines through any given point. For any point $P = (\alpha, \beta)$, there are 2^r distinct lines passing through P, corresponding to the elements of $\mathbb{F}_{2^r}$. Thus the availability is $2^r - 1$, since we only consider non-tangent lines and we are working over $\mathbb{F}_{2^r}$. Note they intersect only at points associated with the erasure.

Now we show a lower bound on the minimum distance. We utilize the approach given in [18]. If $c \in \mathcal{C}$ is a codeword with a nonzero symbol c_i in the i^{th} position corresponding to a point P, then $f_c(P) \neq 0$. The position i has $2^r - 1$ disjoint recovery sets as we showed above, each of which has at least one corresponding nonzero symbol in c. Thus, any nonzero codeword must have nonzero entries in at least 2^r nonzero positions. ■

We proceed now to discuss the distinctness of norm-trace-lifted codes from other classes of codes whose construction involves norm-trace curves.

One-point norm-trace codes

Consider one-point norm-trace codes over $\mathbb{F}_{2^r}$. We show that for $m \leq 2^{2r-2} - 3 \cdot 2^{r-1}$ the one-point norm-trace codes offer the locality from norm-trace curves. We prove that when this is the case, that the basis for one-point norm-trace codes is distinct from norm-trace-lifted codes, and so the codes themselves are distinct.

Proposition 2.19. *Let $\mathcal{X}_{2,r}$ be the norm-trace curve over $\mathbb{F}_{2^r}$, and let $r > 2$. For $m \leq$*

$2^{2r-2} - 3 \cdot 2^{r-1}$,

$$\mathcal{L}(mP_\infty) \neq \mathcal{F}.$$

Proof. Let $x^a y^b \in \mathcal{L}(mP_\infty)$. Recall that the basis for $\mathcal{L}(mP_\infty)$ consists of monomials $x^a y^b$ where

$$a2^{r-1} + b\,(2^r - 1) \leq m.$$

Let $m \leq 2^{2r-2} - 3 \cdot 2^{r-1}$; we show that for $x^a y^b \in \mathcal{L}(mP_\infty)$, $x^a y^b \in \mathcal{F}$. To do so, we show that $a + b < 2^{r-1} - 2$ with the following string of inequalities.

$$a + b \leq a + 2b - \frac{b}{2^{r-1}} = \frac{a2^{r-1} + b2^r - b}{2^{r-1}} \leq \left\lfloor \frac{2^{2r-2} - 3 \cdot 2^{r-1}}{2^{r-1}} \right\rfloor = \left\lfloor 2^{r-1} - 3 \right\rfloor < 2^{r-1} - 2.$$

Therefore, if $m \leq 2^{2r-2} - 3 \cdot 2^{r-1}$, then all monomials $x^a y^b \in \mathcal{L}(mP_\infty)$ are in the set $\mathcal{F}$, and thus we have that $\mathcal{L}(mP_\infty) \subseteq \mathcal{F}$.

To see that these two sets are not equal, observe that $y^{2^{r-1}-3} \in \mathcal{F}$. However, for a monomial y^b to be in $\mathcal{L}(mP_\infty)$,

$$b \leq \left\lfloor \frac{2^{2r-2} - 3 \cdot 2^{r-1}}{2^r - 1} \right\rfloor \leq 2^{r-2} - 2,$$

because $m \leq 2^{2r-2} - 3 \cdot 2^{r-1}$. As

$$2^{r-2} - 2 < 2^{r-1} - 3$$

when $r > 2$, $y^{2^{r-1}-3} \notin \mathcal{L}(mP_\infty)$. Therefore $\mathcal{L}(mP_\infty) \neq \mathcal{F}$. ■

In conclusion, the sets of evaluation polynomials $L(mP_\infty)$ for one-point norm-trace codes are distinct from the set of evaluation polynomials for $\mathcal{F}$ for norm-trace-lifted codes. Further, the extent to which the basis monomials differ can visually be seen in Section 2.4.

Geil's codes $\tilde{E}(s)$

One of the first constructions of codes from norm-trace curves was given by Geil in [9]. There are two sets of codes detailed in [9], the codes $E(s)$ and the codes $\tilde{E}(s)$. The construction uses the more general Miura-Kamiya curves, and then details the particular case of norm-trace curves. We follow that structure here, where we give the definitions for the more general construction, followed by applications to norm-trace curves in particular.

Let a and b be relatively prime, $\mu \neq 0$, and $F'(x,y)$ be such that any monomial $x^\alpha y^\beta$ in the support of $F'(x,y)$ satisfies $\alpha b + \beta a < ab$. Consider the Miura-Kamiya curve given by

$$F(x,y) \coloneqq x^a - \mu y^b - F'(x,y) \in \mathbb{F}_q[x,y].$$

Define the ideal

$$J \coloneqq \langle F(x,y), x^q - x, y^q - y \rangle \subseteq \mathbb{F}_q[x,y].$$

Denote the factor ring $R = \mathbb{F}_q[x,y]/J$. Consider the variety $\{P_1, \ldots, P_n\} = \{P : F(P) = 0\} \subseteq \mathbb{F}_q^2$. It is well-known that the map $\varphi : R \to \mathbb{F}_q^n$ given by

$$\varphi(H + J) \coloneqq (H(P_1), \ldots, H(P_n))$$

is well-defined and is an isomorphism [7].

Geil considers codes with basis B that are constructed by considering images of φ of certain subspaces of R. Lastly, let $\mathcal{M}(x_1, \ldots, x_m)$ denote the set of monomials in the variables $x_1, \ldots, x_m$.

Definition 2.20. Given positive integers a, b let $\prec_w$ denote the *weighted graded ordering* on $\mathcal{M}(x,y)$ defined as follows. We have $x^\alpha y^\beta \prec_w x^\gamma y^\delta$ if and only if one of the following

conditions holds:

1. $\alpha b + \beta a < \gamma b + \delta a$, or

2. $\alpha b + \beta a = \gamma b + \delta a$ and $\beta < \delta$.

Definition 2.21. Let K be a field and let $I \subseteq K[x_1, \ldots, x_m]$ be an ideal. Given a monomial ordering $\prec$ on $\mathcal{M}(x_1, \ldots, x_m)$, the set

$$\Delta_{\prec}(I) \coloneqq \{x_1^{\alpha_1} \ldots x_m^{\alpha_m} : x_1^{\alpha_1} \ldots x_m^{\alpha_m} \text{ is not a leading monomial of any polynomial in } I\}$$

is called the *footprint of I with respect to $\prec$*.

We may now define the codes $E(s)$ and $\tilde{E}(s)$. Denote $\mathbb{N}_0$ the non-negative integers.

Definition 2.22. Let $\rho : \mathcal{M}(x, y) \to \mathbb{N}_0$ be the map given by

$$\rho(x^i y^j) \coloneqq bi + aj.$$

For $s \in \mathbb{N}_0$ define

$$L_s \coloneqq \operatorname{span}_{\mathbb{F}_q}\{M + J : M \in \Delta_{\prec_w}(J), \rho(M) \leq s\}.$$

Define the code

$$E(s) \coloneqq \varphi(L_s).$$

Definition 2.23. Let $D : \mathcal{M}(x, y) \to \mathbb{N}_0$ be the map given by

$$D(x_i y_j) \coloneqq \min\{bq - (b - j)(q - i), aq - (a - i)(q - j), bi + aj\}.$$

For $s \in \mathbb{N}_0$ define

$$K_s \coloneqq \operatorname{span}_{\mathbb{F}_q}\{M + J : M \in \Delta_{\prec_w}(J), D(M) \leq s\}.$$

Define the code

$$\tilde{E}(s) \coloneqq \varphi(K_s).$$

An instance of this more general construction of Geil uses a norm-trace curve, where

$$F(x, y) = x^{\frac{q^r-1}{q-1}} - y^{q^{r-1}} - \cdots - y^q - y.$$

With $F(x, y)$ set, the codes $E(s)$ are one-point norm-trace codes $C_{\mathcal{L}}(D, sP_\infty)$, discussed previously. It remains to detail the codes $\tilde{E}(s)$. In this section, we show by comparing asymptotic rates that the codes $\tilde{E}(s)$ are distinct from norm-trace-lifted codes. To do so, we note [9, Example 5] deals specifically with the rates of the codes $\tilde{E}(s)$ from norm-trace curves when $q = 2$.

Proposition 2.24. *[9, Example 5] Let $\tilde{E}(s)$ be defined with $F(x, y)$ the norm-trace curve and $q = 2$. If r is large, then the rate*

$$\frac{k}{n} \approx 1 - \frac{d}{n} + \frac{d}{n} \ln\left(\frac{d}{n}\right).$$

Proof. Considering Definition 2.23, we see that for $x^i y^j \in \Delta_{\prec_w}(J)$ that

$$D(x^i y^j) = \begin{cases} bi + aj & \text{for } i \leq q^r - a \\ bi + q^r j - ij & \text{for } i > q^r - a \end{cases}.$$

Thus, as $q = 2$, all but a negligible number of elements $x^i y^j \in \Delta_{\prec_w}(J)$ satisfy $D(x^i y^j) =$

$2^{r-1}i + 2^r j - ij$, that is, all but a negligible number of elements satisfy

$$j = \frac{D(x^i y^j) - 2^{r-1}i}{2^r - i}.$$

Therefore, if r is large and s satisfies $0 \leq s \leq D(x^{2^r-2}) = n - 2^r$, then the dimension k of $\tilde{E}(s)$ is approximately

$$\int_0^{\frac{s}{2^{r-1}}} \frac{s - 2^{r-1}i}{2^r - i} di = n - d + d \cdot \ln\left(\frac{d}{n}\right).$$

Thus the rate of $\tilde{E}(s)$ is

$$\frac{k}{n} \approx 1 - \frac{d}{n} + \frac{d}{n} \ln\left(\frac{d}{n}\right)$$

when r is large. ■

We now prove the main proposition of this section, the statement that the two families of codes are distinct.

Proposition 2.25. *The codes $\tilde{E}(s)$ are distinct from norm-trace-lifted codes.*

Proof. By Theorem 2.18, the minimum distance of norm-trace-lifted codes satisfies $d \geq 2^r$, and these codes have length $n = 2^{2r-1}$. By Proposition 2.24, for large r the rate of $\tilde{E}(s)$ is

$$\frac{k}{n} \approx 1 - \frac{d}{n} + \frac{d}{n} \cdot \ln\left(\frac{d}{n}\right).$$

If these two codes are equivalent, then

$$1 - \frac{d}{n} + \frac{d}{n} \ln\left(\frac{d}{n}\right)$$

will asymptotically be 0.25 as r goes to infinity. We consider the following two cases: that

where the expression for minimum distance d contains a term of 2^{2r+s}, and the case where it is not.

Case 1: Suppose that $d = f(r)$ and does not contain a term of the form 2^{2r+s} for some number s. Then, $f(r)$ divided by the length 2^{2r-1} trends towards zero as r goes to infinity, and then

$$\frac{k}{n} \approx 1 - \frac{f(r)}{2^{2r-1}} + \frac{f(r)}{2^{2r-1}} \cdot \ln\left(\frac{f(r)}{2^{2r-1}}\right) \to 1 \text{ as } r \to \infty.$$

Since Theorem 2.17 implies that the asymptotic rate for the lifted codes is 0.25, we have in this case that the codes are distinct.

Case 2: Suppose that d contains a term of the form 2^{2r+s} for some number s. The minimum distance d can not exceed the length n, implying $s \leq -1$. We write $d = 2^{2r+s} + f(r)$. Since $f(r)$ divided by the length 2^{2r-1} trends towards zero as r goes to infinity, and because 2^{2r+s} divided by the length does not trend towards zero as r goes to infinity, that

$$\begin{aligned}
\frac{k}{n} &\approx 1 - \frac{2^{2r+s} + f(r)}{2^{2r-1}} + \frac{2^{2r+s} + f(r)}{2^{2r-1}} \cdot \ln\left(\frac{2^{2r+s} + f(r)}{2^{2r-1}}\right) \\
&= 1 - \left(\frac{2^{2r+s}}{2^{2r-1}} + \frac{f(r)}{2^{2r-1}}\right) + \left(\frac{2^{2r+s}}{2^{2r-1}} + \frac{f(r)}{2^{2r-1}}\right) \cdot \ln\left(\frac{2^{2r+s}}{2^{2r-1}} + \frac{f(r)}{2^{2r-1}}\right) \\
&= 1 - \frac{2^{2r+s}}{2^{2r-1}} - \frac{f(r)}{2^{2r-1}} + \frac{2^{2r+s}}{2^{2r-1}} \cdot \ln\left(\frac{2^{2r+s}}{2^{2r-1}} + \frac{f(r)}{2^{2r-1}}\right) + \frac{f(r)}{2^{2r-1}} \cdot \ln\left(\frac{2^{2r+s}}{2^{2r-1}} + \frac{f(r)}{2^{2r-1}}\right) \\
&\to 1 - 2^{s+1} + 2^{s+1} \cdot \ln(2^{s+1}) \text{ as } r \to \infty
\end{aligned}$$

Note that for $s \leq -1$ that $1 - 2^{s+1} + 2^{s+1} \cdot \ln(2^{s+1})$ is an increasing function, and that for any integer value of $s \leq -1$, that $1 - 2^{s+1} + 2^{s+1} \cdot \ln(2^{s+1}) \neq 0.25$, which is the known asymptotic rate of the norm-trace-lifted codes. Thus, in this case as well, the codes $\tilde{E}(s)$ are not equivalent to norm-trace-lifted codes. ■

Therefore, we see that the norm-trace-lifted codes are distinct from codes from norm-trace

curves previously considered in the literature.

Codes of Barg, Tamo, and Vlăduţ

Another construction of locally recoverable codes from algebraic curves is present in the work of Barg, Tamo, and Vlăduţ in [2], which is a generalization of the Tamo-Barg codes [29]. This construction is quite general, and the specific case of norm-trace curves is mentioned in a paper by Ballico and Marcolla in [1] on higher Hamming weights. Here we will discuss the general construction presented in [2], and then from [1] discuss the two classes of locally recoverable codes from norm-trace curves. In the construction, r is the locality of the code.

The construction is the following. Let $\mathcal{X}$ and $\mathcal{Y}$ be smooth projective absolutely irreducible curves over a field K. Let $g : \mathcal{X} \to \mathcal{Y}$ be a rational separable map of curves of degree $r+1$. Let the pullback $g^* : K(\mathcal{Y}) \to K(\mathcal{X})$ be the function that acts on $K(\mathcal{Y})$ by $g^*(f)(P) = f(g(P))$, where $f \in K(\mathcal{Y})$ and P is a point on $\mathcal{X}$. The map g^* defines a field embedding $K(\mathcal{Y}) \hookrightarrow K(\mathcal{X})$, and we identify $K(\mathcal{Y})$ with its image $g^*(K(\mathcal{Y})) \subset K(\mathcal{X})$.

Since g is separable, the primitive element theorem implies that there exists a function $f \in K(\mathcal{X})$ such that $K(\mathcal{X}) = K(\mathcal{Y})(f)$, and satisfies the equation

$$x^{r+1} + b_r x^r + \cdots + b_0 = 0,$$

where $b_i \in K(\mathcal{Y})$. The function f can be considered as a map $f : \mathcal{X} \to \mathbb{P}^1_K$, and we denote its degree $\deg(f)$ by h.

Let $S = \{P_1, \ldots, P_s\} \subset \mathcal{Y}(K)$ be a subset of $\mathbb{F}_q$-rational points of $\mathcal{Y}$ and let D be a positive divisor of degree $\ell \geq 1$ whose support is disjoint from S. Assume that for S and g that

$$A \coloneqq g^{-1}(S) = \{P_{ij} : i = 0, \ldots, r, \text{ and } j \in [s]\} \subseteq \mathcal{X}(K),$$

$$g(P_{ij}) = P_j \text{ for all } i, j,$$

and

$$b_i \in \mathcal{L}(n_i D) \text{ for } i = 0, 1, \ldots, r,$$

for some natural numbers n_i.

Let $\{f_1, \ldots, f_m\}$ be a basis for $\mathcal{L}(D)$. The functions $f_i \in K(\mathcal{Y})$, and thus are constant on the fibers of the map g, analagous to the good polynomials g of the Tamo-Barg construction. Consider the K-subspace V of $K(\mathcal{X})$ of dimension rm generated by the functions

$$\{f_j \cdot f^i : i = 0, \ldots, r-1, \text{ and } j \in [m]\}.$$

Since D is disjoint from S, the evaluation map given by

$$\begin{aligned} ev: \quad V &\to & K^{(r+1)s} \\ F &\mapsto & (F(P_{ij}), i = 0, \ldots, r-1, j \in [m]) \end{aligned}$$

is well-defined. The code $C(D, g) \coloneqq ev(F) \subseteq \mathbb{F}_q^{(r+1)s}$ is the image of this evaluation map.

The work of Ballico and Marcolla discusses two classes of locally recoverable codes from norm-trace curves over $\mathbb{F}_{q^r}$ that result from this construction in [1, Remark 1]. The distinctness of each of these codes from norm-trace-lifted codes is addressed below.

- The first family of codes in [1, Remark 1] are $[q^{2r-1}, (t+1)(q^{r-1}-1), q^{r-1}-1]$ codes. They are distinct from norm-trace-lifted codes, because with $q = 2$, they have minimum distance $2^{r-1}-1$. This minimum distance is strictly smaller than the minimum distance of at least 2^r for norm-trace-lifted codes which is shown in Theorem 2.18.
- The second family in [1, Remark 1] are $[q^{2r-1}-q^{r-1}, (t+1)(q+\cdots+q^{r-1}), q+\cdots+q^{r-1}]$ codes. They are distinct from norm-trace-lifted codes, because with $q = 2$, they have a

length of $2^{2r-1} - 2^{r-1}$. This length is strictly less than the length of norm-trace-lifted codes, as norm-trace-lifted codes utilize all 2^{2r-1} affine points on the norm-trace curve.

Thus, neither of the codes discussed in [1] are equivalent to norm-trace-lifted codes.

Codes of Bartoli, Montanucci, and Quoos

The code construction of Bartoli, Montanucci, and Quoos in [3] uses facts about intersection properties of automorphism subgroups to construct locally recoverable codes. In this work, only one class of codes from norm-trace curves is described, and these codes are also distinct from norm-trace-lifted codes.

Let $F/\mathbb{F}_q$ be a function field of genus g. Consider s subgroups H_i of the automorphism group of $F/\mathbb{F}_q$, each of sizes $r_i + 1$, such that the group $G \simeq \bigotimes_{i=1}^{s} H_i$ is isomorphic to the internal direct product of $H_1, \ldots, H_s$. Let $\mathcal{P}$ be a set of places in F lying over m rational places in the fixed field F^G that are completely split in the extension F/F^G. Define

$$n = m \prod_{i=1}^{s} (r_i + 1),$$

that is, n to be the total number of places of F lying over the m selected rational places in F^G.

Suppose that there exists a place P_∞ of F which is totally ramified in F/F^G and let $Q_\infty^{(i)}$ be the unique place in F^{H_i} lying under P_∞. For $i \in [s]$ suppose there exist functions z_i, q_i such that

1. $z_i \in F^{H_i}$ and $\text{supp}((z_i)_\infty) = \{Q_\infty^{(i)}\}$,

2. $w_i \in F \backslash F^{H_i}$ and $\text{supp}((w_i)_\infty) = \{P_\infty\}$,

3. $w_i : \mathcal{P}^{H_i} \to \mathbb{F}_q$ is injective.

For each $i \in [s]$, let $t_i \geq 1$ be such that

$$V_i \coloneqq \left\{ \sum_{\ell=0}^{r_i-1} \left(\sum_{j=0}^{t_i} a_{\ell j}^{(i)} z_i^j \right) w_i^\ell \in F : a_{\ell j}^{(i)} \in \mathbb{F}_q \right\}$$

is contained in $\mathcal{L}((n-d)P_\infty)$ for some $1 \leq d \leq n$ and let $V = \bigcap_{i=1}^s V_i \subset \mathcal{L}((n-d)P_\infty)$. If $\dim_{\mathbb{F}_q}(V) > 0$, then there exists an

$$[n, \dim_{\mathbb{F}_q}(V), \geq d]$$

locally recoverable code.

The codes in [3, Section IV-E] are those which consider the specific case of the norm-trace curve over $\mathbb{F}_{q^\ell}$. They consider the following subgroups of the automorphism group of the norm-trace function field:

$$H_1 \coloneqq \left\{ (x, y) \mapsto (x + a, y) : \sum_{i=0}^{\ell-1} a^{q^i} = 0, a \in \mathbb{F}_q \right\},$$

$$H_2 \coloneqq \left\{ (x, y) \mapsto (x, \lambda y) : \lambda \in \mathbb{F}_{q^\ell} \text{ and } \lambda^{\frac{q^\ell - 1}{q-1}} = 1 \right\}.$$

With the subgroups H_1 and H_2, we define the following codes.

Proposition 2.26. *Let $0 \leq t_1$, and $i = 1, 2$ satisfying*

$$S = M_1 q + M_2(q^\ell - 1) \leq q^{\ell-1}(q^\ell - 1)$$

for

$$M_1 = \max\left\{ t_1, \frac{q^\ell - 1}{q-1} - 2 \right\} \text{ and } M_2 = \max\{t_2, q^{\ell-1} - 2\}.$$

Choosing

$$m_1 = \min\left\{t_1, \frac{q^\ell - 1}{q-1} - 2\right\} \text{ and } m_2 = \min\{t_2, q^{\ell-1} - 2\},$$

there exists a $[q^{2\ell-1} - q^{\ell-1}, (m_1+1)(m_2+1), q^{2\ell-1} - q^{\ell-1} - S]$ *locally recoverable code over* $\mathbb{F}_{q^\ell}$.

The codes from norm-trace codes in Proposition 2.26 differ from norm-trace-lifted codes in multiple ways. Not only do they have a much smaller minimum distance of $2^{\ell-1} - 1$, but they also have length of $2^{2\ell-1} - 2^{\ell-1}$, shorter than norm-trace-lifted codes.

2.4 Comparisons

Rate comparison to one-point norm-trace codes

In Section 2.3, we saw that one-point norm-trace codes are distinct from the norm-trace-lifted codes defined here. A natural question is then, since they are distinct, how do their asymptotic rates compare.

Determining the asymptotic rate of one-point Hermitian codes in [18] uses the fact that

$$\frac{m + 1 - g + \dim \mathcal{L}(K - mP_\infty)}{q^3} \leq \frac{m+1}{q^3} \to 0 \text{ as } q \to \infty$$

for a canonical divisor K of the Hermitian function field $\mathcal{X}_q$. This bound is sufficient to completely determine the asymptotic rate for one-point Hermitian codes, because the upper bound given goes to zero as the field size increases.

To find the dimension of the one-point norm-trace code, we must count all pairs (a, b) with a and b non-negative, and $a2^{r-1} + b(2^r - 1) \leq 2^{2r-2} - 3 \cdot 2^{r-1}$. To start, recall from

Section 2.3 that for a monomial $x^a y^b \in \mathcal{L}(mP_\infty)$, $b \leq 2^{r-2} - 2$. Similarly we can find that $a \leq 2^{r-1} - 3$. The desired integer pairs are those within the triangle formed by the points $(0,0)$, $(2^{r-1}-3, 0)$, and $(0, 2^{r-2}-2)$. Taking a slightly larger triangle gives a slight overestimate for the dimension, but does not affect the asymptotic result.

Proposition 2.27. *The rate of one-point norm-trace codes $C_{\mathcal{L}}(D, mP_\infty)$ with $m \leq 2^{2r-2} - 3 \cdot 2^{r-1}$ defined over $\mathbb{F}_{2^r}$ is asymptotically* 0.125.

Proof. To find the dimension, we wish to find integer solutions within the triangle formed by $(0,0)$, $(2^{r-1}-2, 0)$, and $(0, 2^{r-2}-1)$. By Pick's theorem, for a plane polygon with integer vertices,

$$A = i + \frac{b}{2} - 1$$

where A is the area of the figure, i the number of interior integer points, b the number of boundary integer points. Because distinct monomials yield linearly independent codewords by Lemma 2.14, and there are $i + b$ such monomials, the goal is to determine $i + b$.

First, the number of boundary points is $(2^{r-1} - 2) + (2^{r-2} - 1)$ plus the number of points on the diagonal of the triangle. The number of integer points on the segment connecting the points $(2^{r-1} - 2, 0)$ and $(0, 2^{r-2} - 1)$ is simply the greatest common divisor of the two non-zero components given, which is $2^{r-2} - 1$, and so we gain an additional $2^{r-2} - 3$ boundary integer points, giving a total of

$$(2^{r-1} - 2) + (2^{r-2} - 1) + 2^{r-2} - 3 = 2^r - 6$$

integer points on the boundary.

The area of the figure is just the area of a triangle, so

$$A = \frac{1}{2}\left(2^{r-2}-1\right)\left(2^{r-1}-2\right) = 2^{2r-4} - 2^{r-1} + 1.$$

With these two above calculations of A and b, we find the number of interior points to be

$$i = A - \frac{b}{2} + 1 = (2^{2r-4} - 2^{r-1} + 1) - \left(\frac{2^r - 6}{2}\right) + 1 = 2^{2r-4} - 2^r + 5,$$

and so the dimension is upper bounded by

$$i + b = 2^{2r-4} - 1.$$

We can also see that asymptotically, the boundary points do not add much to the dimension. With that observation, we finally have the rate of the code is asymptotically

$$\frac{2^{2r-4}-1}{2^{2r-1}} = \frac{1}{2^3} - \frac{1}{2^{2r-1}} \to \frac{1}{8} \text{ as } r \to \infty.$$

■

The results of the above proof can be seen visually in Figures 2.4 and 2.5.

Basis monomial and good monomial comparisons

In the Hermitian case, the good monomials with $a + b$ less than the locality q were exactly those which formed the basis for the one-point Hermitian codes. Monomials with $a + b > q$ were needed to guarantee that the associated code rate is asymptotically nonzero. This can be seen in Figures 2.2 and 2.3.

Note that in all of the figures in this section, a is on horizontal axis.

This is in contrast with the norm-trace-lifted codes, where the good monomials with $a+b$ less than the locality of $2^{r-1}-2$ are the only good monomials, but still yield good asymptotic rate results. This can be seen in Figures 2.4 and 2.5.

This triangular shape, justified by Lemma 2.17, is slightly different from what is observed in the Hermitian case, where the monomials with $a+b$ greater than the locality were necessary for good rate results.

We may also compare the two lifted codes, shown in Figures 2.6 and 2.7; with these graphics we can see why the rate results for the norm-trace-lifted codes may be much better than those for Hermitian-lifted codes.

General tables

We compare the parameters of these norm-trace-lifted codes to the Hermitian-lifted codes of [18]. Table 2.4 makes comparison with consistent alphabet size, that is, $q^2 = 2^r$. We also list one-point Hermitian codes $C_{\mathcal{L}}(P_1 + \cdots + P_{q^2}, mP_\infty)$ with pole allowance $m \leq q^2 - 1$ and one-point norm-trace codes $C_{\mathcal{L}}(P_1 + \cdots + P_{2^{2r-1}}, mP_\infty)$ with pole allowance $m \leq 2^{2r-2} - 3 \cdot 2^{r-1}$.

We also introduce another relevant metric.

Definition 2.28. The relative locality ρ of a code is defined to be the locality of the code divided by the length of the code, that is,

$$\rho = \frac{d}{n}.$$

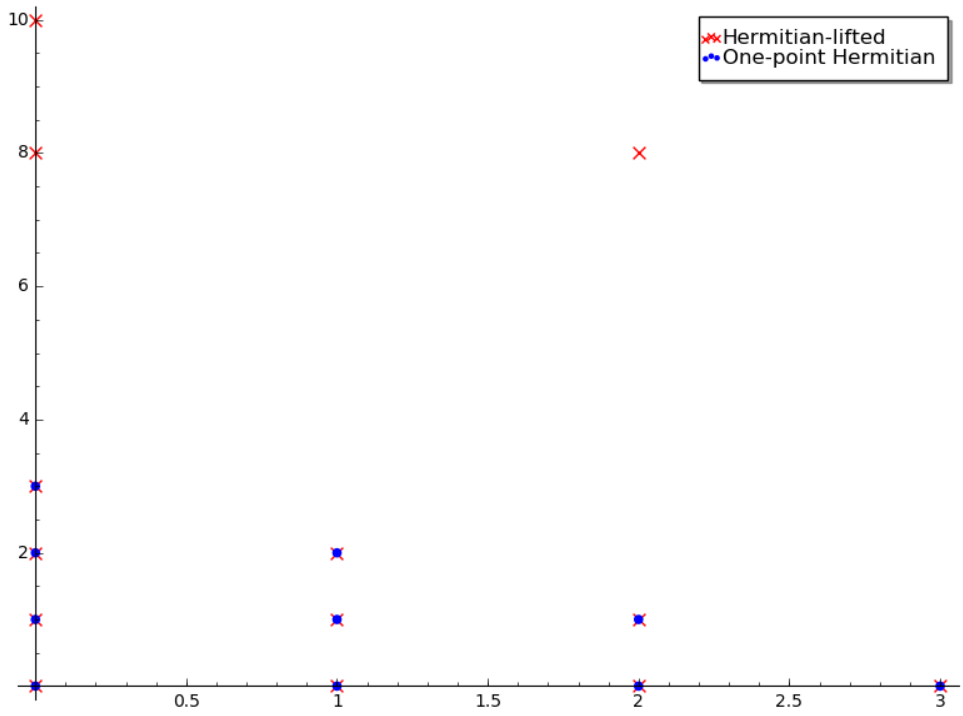

Figure 2.2: One-point Hermitian code compared with HLC when $q = 4$ (over $\mathbb{F}_{16}$).

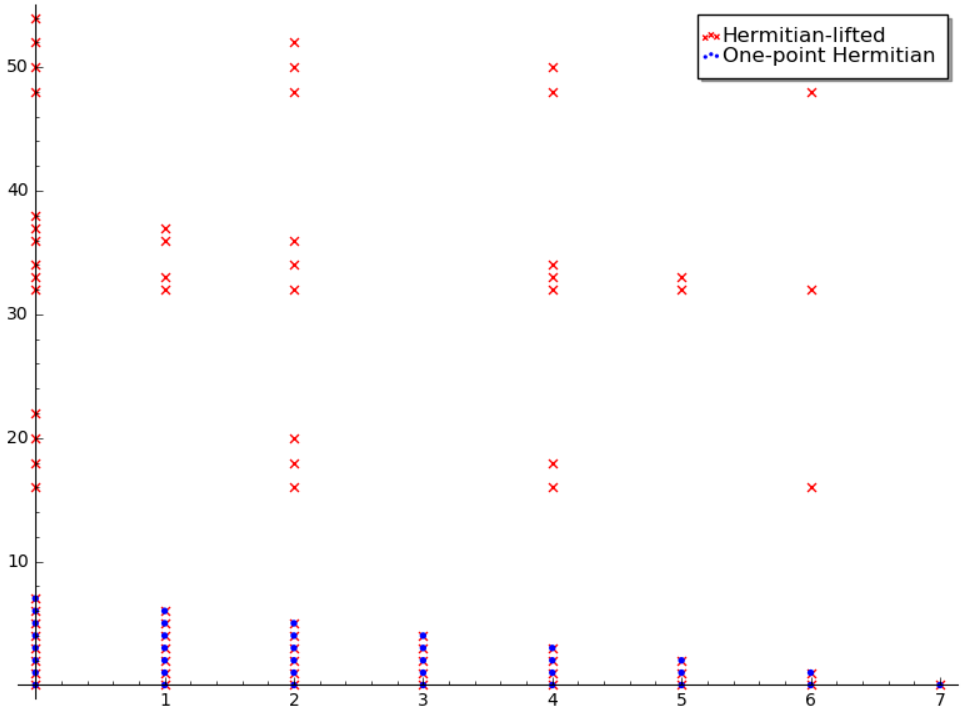

Figure 2.3: One-point Hermitian code compared with HLC when $q = 8$ (over $\mathbb{F}_{64}$).

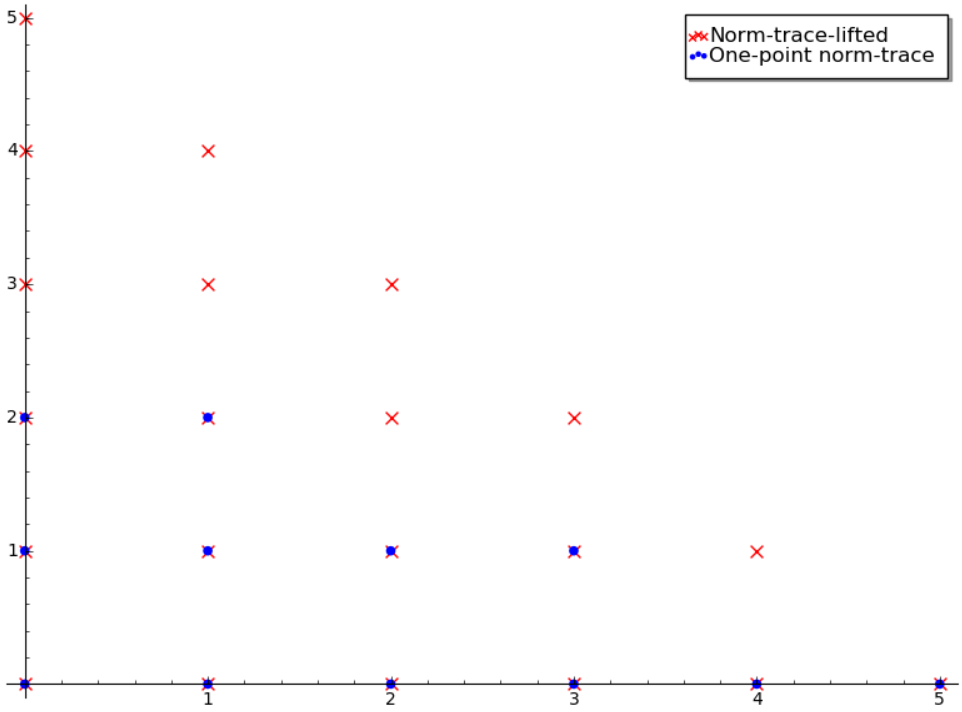

Figure 2.4: One-point norm-trace code compared with NTLC when $r = 4$ (over $\mathbb{F}_{16}$).

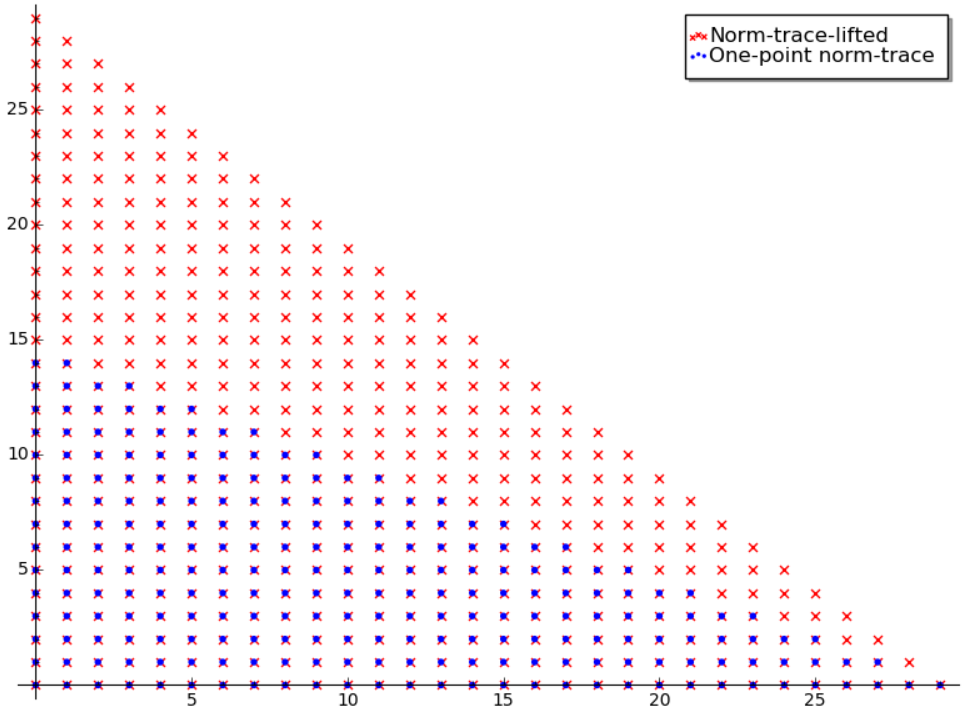

Figure 2.5: One-point norm-trace code compared with NTLC when $r = 6$ (over $\mathbb{F}_{64}$).

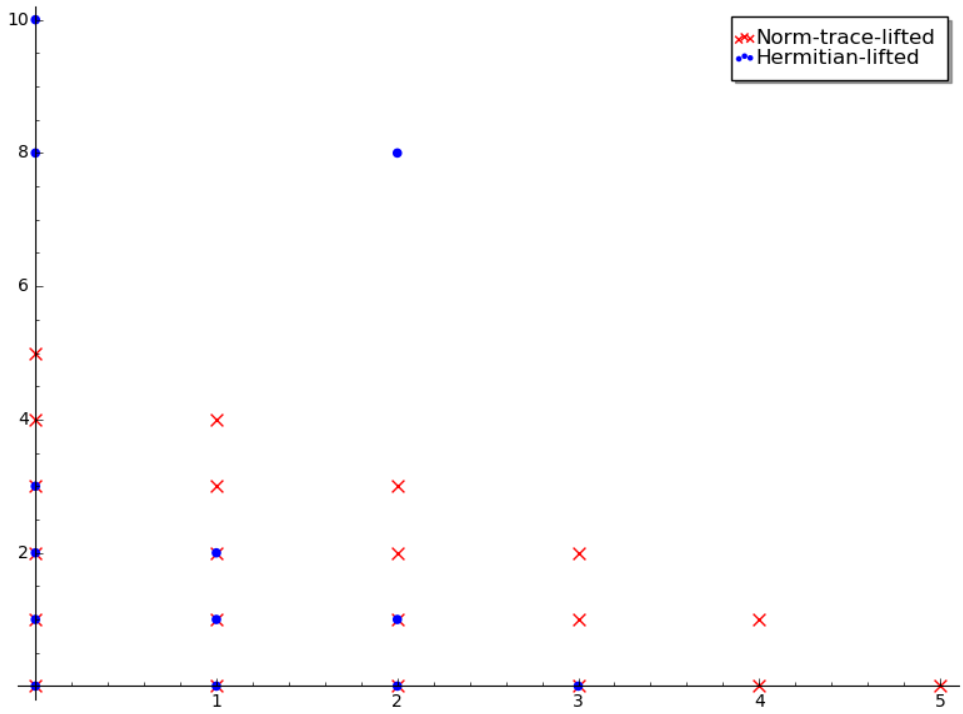

Figure 2.6: HLC compared with NTLC when $q = 4$ and $r = 4$ respectively (over $\mathbb{F}_{16}$).

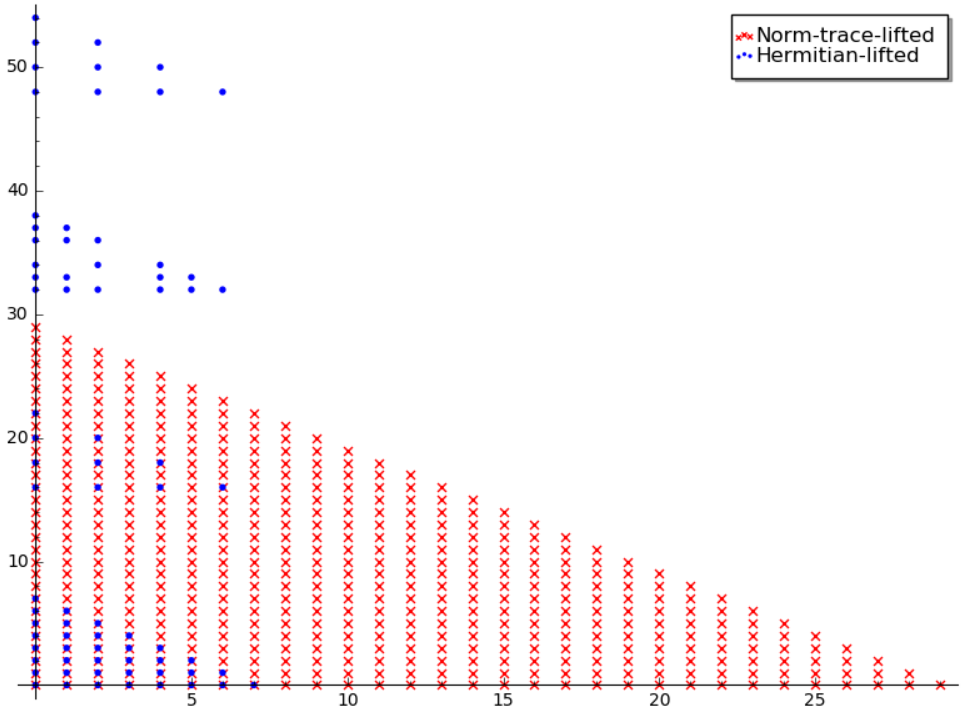

Figure 2.7: HLC compared with NTLC when $q = 8$ and $r = 6$ respectively (over $\mathbb{F}_{64}$).

Table 2.5 compares the Hermitian-lifted codes with the norm-trace-lifted codes based on their locality; since the locality of the Hermitian-lifted codes are q and the locality of the norm-trace-lifted codes are $2^{r-1}-2$, to make the two comparable we consider when $q = 2^{r-1}$.

Table 2.4: One-point codes versus lifted codes comparisons, general

	One-point Hermitian code	One-point Norm-trace code	HLC	NTLC
Alphabet size	2^r	2^r	2^r	2^r
Locality	$2^{r/2}$	$2^{r-1}-2$	$2^{r/2}$	$2^{r-1}-2$
Availability	2^r-1	2^r-1	2^r-1	2^r-1
Length	$2^{3r/2}$	2^{2r-1}	$2^{3r/2}$	2^{2r-1}
Dimension	$\leq 2^r$	$\leq 2^{2r-4}-1$	$\geq 0.007 \cdot 2^{3r/2}$	$(0.25-\varepsilon_r)\cdot 2^{2r-1}$
Rate	$\frac{1}{2^{r/2}}$	$\leq \frac{1}{8}-\frac{1}{2^{2r-1}}$	≥ 0.007	$0.25-\varepsilon_r$
Min. dist.	See [26, 31]	See [9]	$2^r \leq d$	$2^r \leq d$
Rel. Locality	$\frac{1}{2^r}$	$\frac{1}{2^r}-\frac{1}{2^{2r-2}}$	$\frac{1}{2^r}$	$\frac{1}{2^r}-\frac{1}{2^{2r-2}}$

Table 2.5: Lifted code comparisons, general

	HLC	NTLC
Locality	2^{r-1}	$2^{r-1}-2$
Alphabet Size	2^{2r-2}	2^r
Availability	$2^{2r-2}-1$	2^r-1
Length	2^{3r-3}	2^{2r-1}
Dimension	$\geq 0.007 \cdot 2^{3r-3}$	$(0.25-\varepsilon_r)\cdot 2^{2r-1}$
Rate	≥ 0.007	$0.25-\varepsilon_r$
Min. Dist.	$2^{2r-2} \leq d$	$2^r \leq d$

Specific values of r

Consider norm-trace-lifted codes $\mathcal{C}_{\mathcal{X}_{2,r}}$ defined over $\mathbb{F}_{2^r}$. Tables 2.6, 2.7, and 2.8 take specific instances of values of r, and are analogues to Table 2.4. The value of r used in each table is noted in the top left block. These three tables specifically showcase comparisons based on consistent alphabet size.

Note that the rates on the one-point norm-trace codes $C_{\mathbb{L}}(D, mP_\infty)$ are given by taking the minimum value that m must be for the minimum distance to be nontrivial. Also, exact

values for the dimensions and rates of the Hermitian-lifted codes are taken from Section 4 of [18].

Tables 2.9, 2.10, and 2.11 contain comparisons among Hermitian-lifted codes and norm-trace-lifted codes based on similar locality, and are analogues to Table 2.5. Again, exact values for the dimensions and rates of the Hermitian-lifted codes are taken from Section 4 of [18].

Note that there was no explicit computation done in [18] when $r = 8$, i.e. when $q = 2^7 = 128$, and so the table with $r = 8$ contains only bounds for the Hermitian-lifted codes.

2.5 Sporadic good monomials

It was discussed that the Hermitian-lifted codes required monomials $x^a y^b$ with $a + b$ greater than the locality to have rate bounded away from zero; we shall call these sporadic, since their pattern is yet to be determined.

Definition 2.29. Let $\mathcal{X}$ be an algebraic curve such that $|L_{\alpha,\beta} \cap \mathcal{X}| \geq \ell$ for all non-tangent lines $L_{\alpha,\beta}$, and consider the curve-lifted code $\mathcal{C}_{\mathcal{X}}$ constructed from $\mathcal{X}$ with locality ℓ. We call a good monomial $x^a y^b$ for $\mathcal{C}_{\mathcal{X}}$ *sporadic* if $a + b > \ell$.

However, monomials with $a + b > 2^{r-1} - 2$ are not needed to guarantee that the associated norm-trace-lifted code rate is asymptotically nonzero. Consider the two cases, the Hermitian case and the norm-trace case with $q = 2$, compared in the Table 2.12.

From Table 2.12 we might infer that, in general, the difference seems to be that the locality for the norm-trace-lifted codes is strictly less than the second-highest degree of any term in the defining curve equation. Specifically, the second-highest degree in the Hermitian curve equation $x^{q+1} = y^q + y$ is q, and q is exactly the locality of the Hermitian-lifted codes. This

Table 2.6: One-point codes versus lifted codes over $\mathbb{F}_{16}$

$(r = 4)$	Hermitian code	Norm-trace code	HLC	NTLC
Alphabet size	16	16	16	16
Locality	4	6	4	6
Availability	15	15	15	15
Length	64	128	64	128
Dimension	≤ 16	12	13	21
Rate	$\leq \frac{1}{4} = 0.250$	$\leq \frac{12}{128} \sim 0.094$	$\frac{13}{64} \sim 0.203$	$\frac{21}{128} \sim 0.164$
Min. dist.	See [26, 31]	See [9]	$16 \leq d$	$16 \leq d$
Rel. Locality	$\frac{1}{16}$	$\frac{1}{16} - \frac{1}{64}$	$\frac{1}{16}$	$\frac{1}{16} - \frac{1}{64}$

Table 2.7: One-point codes versus lifted codes over $\mathbb{F}_{64}$

$(r = 6)$	Hermitian code	Norm-trace code	HLC	NTLC
Alphabet size	64	64	64	64
Locality	8	30	8	30
Availability	63	63	63	63
Length	512	2048	512	2048
Dimension	≤ 64	240	75	465
Rate	$\leq \frac{1}{8} = 0.125$	$\leq \frac{240}{2048} \sim 0.117$	$\frac{75}{512} \sim 0.146$	$\frac{465}{2048} \sim 0.227$
Min. dist.	See [26, 31]	See [9]	$64 \leq d$	$64 \leq d$
Rel. Locality	$\frac{1}{64}$	$\frac{1}{64} - \frac{1}{1024}$	$\frac{1}{64}$	$\frac{1}{64} - \frac{1}{1024}$

Table 2.8: One-point codes versus lifted codes over $\mathbb{F}_{256}$

$(r = 8)$	Hermitian code	Norm-trace code	HLC	NTLC
Alphabet size	256	256	256	256
Locality	16	126	16	126
Availability	255	255	255	255
Length	4096	32768	4096	32768
Dimension	≤ 256	4032	505	8001
Rate	$\leq \frac{1}{16} \sim 0.063$	$\leq \frac{4032}{32768} \sim 0.123$	$\frac{505}{4096} \sim 0.123$	$\frac{8001}{32768} \sim 0.244$
Min. dist.	See [26, 31]	See [9]	$256 \leq d$	$256 \leq d$
Rel. Locality	$\frac{1}{256}$	$\frac{1}{256} - \frac{1}{16384}$	$\frac{1}{256}$	$\frac{1}{256} - \frac{1}{16384}$

Table 2.9: Lifted code comparisons with locality about 8

$(r = 4)$	HLC	NTLC
Locality	8	6
Alphabet Size	64	16
Availability	63	15
Length	512	128
Dimension	75	21
Rate	$\frac{75}{512} \sim 0.146$	$\frac{21}{128} \sim 0.164$
Min. Dist.	$64 \leq d$	$16 \leq d$

Table 2.10: Lifted code comparisons with locality about 32

$(r = 6)$	HLC	NTLC
Locality	32	30
Alphabet Size	1024	64
Availability	1023	63
Length	32768	2048
Dimension	3675	465
Rate	$\frac{3675}{32768} \sim 0.112$	$\frac{465}{2048} \sim 0.227$
Min. Dist.	$1024 \leq d$	$64 \leq d$

Table 2.11: Lifted code comparisons with locality about 128

$(r = 8)$	HLC	NTLC
Locality	128	126
Alphabet Size	16384	256
Availability	16383	255
Length	2097152	32768
Dimension	≥ 14680	8001
Rate	≥ 0.007	$\frac{8001}{32768} \sim 0.244$
Min. Dist.	$16384 \leq d$	$256 \leq d$

Table 2.12: Comparing HLC and NTLC defining equations

Code	Defining equation	Largest x-power	Largest y-power	Locality
HLC	$x^{q+1} = y^q + y$	$q + 1$	q	q
NTLC	$x^{2^{r-1}} = y^{2^{r-1}} + \cdots + y$	$2^r - 1$	2^{r-1}	$2^{r-1} - 2$

situation is in contrast to the norm-trace-lifted codes, where the second-highest degree term in the norm-trace curve equation is 2^{r-1} and the locality of the code is $2^{r-1}-2$.

We consider a broad class of curves and show that it cannot yield any sporadic monomials. However, to apply this result to a specific curve does require the knowledge of the intersection cardinality between lines and that given curve, which is in general not known.

Theorem 2.30. *Suppose that $\mathcal{X}$ is a curve defined by $p(x,y)=0$ over $\mathbb{F}_q$, where the degree of any monomial $x^a y^b$ on $\mathcal{X}$ is defined to be $a+b$. Call ℓ the locality of the associated curve-lifted code. If the second-highest degree of any term in $p(x,y)$ is greater than ℓ, then there are no sporadic good monomials for the curve-lifted defined by $p(x,y)$.*

Proof. We follow the second half of Lemma 2.17. Take the line $L_{1,0}(t)=(t,t)$, so that $(M_{a,b}\circ L_{1,0})(t)=t^{a+b}$. Then, if $a+b>\ell$, see that

$$\deg_{\alpha,\beta}(t^{a+b})\geq \ell$$

since

$$\widehat{t^{a+b}} = t^{a+b} \bmod p(x,y)$$

is a polynomial with degree no less than the second-highest degree of $p(x,y)$, which we assumed to be greater than the locality. Therefore, no monomial with $a+b>\ell$ can be a sporadic good monomial. ■

All of the above work, however, assumes that we use all non-tangent lines in the space for recovery sets; considering a restricted set of lines to form the recovery sets might yield more beneficial results. Consider again the case of norm-trace-lifted codes. The locality of norm-trace-lifted codes is $2^{r-1}-2$, and the second-highest degree of the defining equation is 2^{r-1}. The intersection $L_{1,0}\cap\mathcal{X}_{2,r}$ any monomial $x^a y^b$ will not restrict to a polynomial with low

enough degree. However, the locality of $2^{r-1}-2$ is defined because any non-horizontal line intersected in at least $2^{r-1}-1$ distinct affine points. In Lemma 2.10 we see that the non-tangent lines intersect in exactly either $2^{r-1}-1$ or $2^{r-1}+1$ points. On lines with intersection number $2^{r-1}-1$, monomials $a^a y^b$ will not restrict to a low degree polynomial.

Alternatively, one may take only the lines that have the bigger intersection number of $2^{r-1}+1$. Computations show that approximately half of the non-horizontal lines intersect the norm-trace curve in $2^{r-1}-1$ points, while the other half intersect in $2^{r-1}+1$ points. If only the latter lines are taken, then it is feasible for a monomial to be good over just the set of lines that intersect in $2^{r-1}+1$ distinct points.

Suzuki-lifted codes

Theorem 2.30 gives criterion for determining if a curve $\mathcal{X}$ yields sporadic good monomials. It depends on knowing the intersection numbers between lines and the curve. This is in general not known. The Suzuki curves are one family of curves where this information is known [14, 19].

Definition 2.31. The *Suzuki curve* over $\mathbb{F}_q$ is defined by the equation

$$\mathcal{X}_n : x^{q_0}(x^q - x) = y^q - y$$

where $q_0 = 2^n$ and $q = 2^{2n+1}$ for some positive integer n.

Remark 2.32. [14] For the Suzuki curve $\mathcal{X}_n$, $|\mathcal{X}_n(\mathbb{F}_q)| = q^2+1$, so there are q^2 affine points on $\mathcal{X}_n$ over $\mathbb{F}_q$.

Proof. It is well-known that for $\alpha \in \mathbb{F}_q$, $\alpha^q = \alpha$. Then for any $P = (\alpha, \beta) \in \mathbb{F}_q^2$,

$$\alpha^{q_0}(\alpha^q - \alpha) = \alpha^{q_0} \cdot 0 = 0 = \beta^q - \beta,$$

and P is a point on the Suzuki curve over $\mathbb{F}_q$. ■

Notice that there are only q^2 affine points in $\mathbb{F}_q^2$; thus, every affine point over $\mathbb{F}_q$ is a point on the Suzuki curve $\mathcal{X}_n$. Therefore, every line $L_{\alpha,\beta}$ over $\mathbb{F}_q$ intersects the Suzuki curve in exactly q affine points, that is, at all q affine points on $L_{\alpha,\beta}$.

We proceed to give relevant definitions for Suzuki-lifted codes. For the following conditions, let $q = 2^{2n+1}$ for some $n \in \mathbb{Z}^+$.

Definition 2.33. Let

$$\mathbb{L} \coloneqq \{L_{\alpha,\beta} : \alpha \in \mathbb{F}_q \backslash \{0\}, \beta \in \mathbb{F}_q\}$$

be the set of lines

$$L_{\alpha,\beta}(t) = (t, \alpha t + \beta).$$

Definition 2.34. For $f \in \mathbb{F}_q[x, y]$ and $g \in \mathbb{F}_q[t]$ and a line $L_{\alpha,\beta} : \mathbb{F}_q \to \mathbb{F}_q^2$, we say that $f \circ L_{\alpha,\beta}$ *agrees with* g *on* $\mathcal{X}_n$, and write

$$f \circ L_{\alpha,\beta} \equiv_{\mathcal{X}_n} g,$$

if $f(L_{\alpha,\beta}(t)) = g(t)$ for all $t \in \mathbb{F}_q$ with $L_{\alpha,\beta}(t) \in \mathcal{X}_n$.

Definition 2.35. Let $\mathcal{F}$ be given by

$$\mathcal{F} \coloneqq \left\{ f \in \mathbb{F}_q[x, y] : \begin{array}{l} \forall L_{\alpha,\beta} \in \mathbb{L}, \exists g \in \mathbb{F}_q[t]_{<q-1} \\ \text{and } f \circ L_{\alpha,\beta} \equiv_{\mathcal{X}_n} g \end{array} \right\}.$$

Definition 2.36. The *Suzuki-lifted code* $\mathcal{C} \subseteq (\mathbb{F}_q)^{q^2}$ is the evaluation code

$$\mathcal{C}_{\mathcal{X}_n} \coloneqq \{(f(x,y))_{(x,y)\in\mathcal{X}_n(\mathbb{F}_q)} : f \in \mathcal{F}\}.$$

Thus, because the intersection number between lines and the Suzuki curve over $\mathbb{F}_q$ is q, we then have the locality is $q-1$. We now apply Theorem 2.30 to the Suzuki curve, in Theorem 2.37.

Theorem 2.37. *There are no sporadic good monomials in the basis for the evaluation functions of a Suzuki-lifted code.*

Proof. Every line contained in $\mathbb{F}_q^2$ is such that every point is also a point on the Suzuki curve. In other words, all q points on any line in $\mathbb{F}_q^2$ are on the Suzuki curve. Therefore, the locality of the Suzuki-lifted code defined over $\mathbb{F}_q$ is $q-1$. Notice that the defining equation for the Suzuki curve may be re-written as

$$\mathcal{X}_n : x^{q_0+q} + y^q - x^{q_0+1} - x = 0.$$

Because $q = 2^{2n+1} > 2^n + 1 = q_0 + 1$ in general, we may see that the second-highest power in the defining equation for the Suzuki curve is q. Since $q-1 < q$, by Theorem 2.30, there can be no good monomials $x^a y^b$ with $a+b \geq q$ in the basis for a Suzuki-lifted code. ■

It is important to note that because the basis functions for the Riemann-Roch spaces from the Suzuki function field are not strictly monomials, Theorem 2.37 does not entirely eliminate Suzuki curves as a good candidate for lifting. The Riemann-Roch $\mathcal{L}(mP_\infty)$ space for the Suzuki function field has the following basis, as described below [14].

The five rational functions on the Suzuki curve $\mathcal{X}$ are

$$f_0 = 1,\ f_q = \frac{y}{u},\ f_{q+q_0} = \frac{z}{u},$$

$$f_{q+2q_0} = f_q^{2q_0+1},\ f_{q+2q_0+1} = f_q f_{q+q_0}^{2q_0} + f_{q+2q_0}^{2q_0}.$$

Define the function f_n by

$$f_n = f_q^{a_1} f_{q+q_0}^{a_2} f_{q+2q_0}^{a_3} f_{q+2q_0+1}^{a_4}$$

where

$$n = a_1 q + a_2(q + q_0) + a_3(q + 2q_0) + a_4(q + 2q_0 + 1)$$

for non-negative integers a_i. Then, the set of functions

$$\{f_n : n \leq m\}$$

is a basis for the space $\mathcal{L}(mP_\infty)$.

This observation means that we may have need to consider good functions generally, outside of good monomials. There may exist good functions which restrict sufficiently and yield linearly independent codewords, but which are composed of monomials which are not good.

2.6 Future research

The first research direction is to find intersection numbers between lines and norm-trace curves in cases other than $q = 2$. If finding exact intersection numbers is not feasible, then at the very least, (relatively) large lower bounds are sufficient. One possible approach may be to turn the problem into an equivalent matrix rank problem, using results such as the

König-Rados theorem [16, Theorem 6.1]. It remains to be proven what $|L_{\alpha,\beta} \cap \mathcal{X}_{q,r}|$ is in general.

Another idea is to disregard certain lines, as suggested in Section 2.5. The elimination of lines with intersection numbers that are too low might have the effect of introducing sporadic good monomials into the basis of the set of evaluation functions, leading to better bounds on the rate of the code. Improvement of the norm-trace-lifted code rate might occur if the recovery sets were a strict subset of non-tangent lines.

Yet another direction is to consider repair groups which are generated by low degree curves other than lines, such as quadratics or cubics. Some work in this direction for Reed-Solomon codes is present in [17]. These may intersect the norm-trace curves in many more affine points than lines, and there exist some results on such intersections already [4, 5]. However, a key consideration is that the desirable disjoint repair group property would most likely be violated, since quadratics and cubics may intersect each other in more than one affine point, unlike lines. We may be able to form some effective repair groups from higher degree curves.

Lastly, it may be interesting to consider other curves in this construction. We discussed quotients of Hermitian curves and quotients of norm-trace curves in Section 2.3, and Suzuki curves in Section 2.5. There may still exist other families of curves which may yield interest results if considered with this lifting procedure.

In further work, we may also consider approaches to prove the following conjectures related to norm-trace-lifted codes. First is a conjecture on the number of points of intersection between lines and norm-trace curves, based on the computational results presented in Tables 2.2 and 2.3.

Conjecture 2.38. *Let $r = 3$ and consider the norm-trace curve over $\mathbb{F}_{q^3}$. The intersection between a line $L_{\alpha,\beta} \in \mathbb{L}$ with $\alpha \neq 0$ and the norm-trace curve $\mathcal{X}_{q,3}$ over $\mathbb{F}_{q^3}$ has cardinality*

of $q^2 + \gamma q + 1$*, where* $\gamma \in \{-1, 0, 1\}$.

By a similar argument as in the latter half of Lemma 2.17, assuming Conjecture 2.38, it can be seen that there are no good monomials with $a + b$ greater than the locality in the case when q is even and $r = 3$. Thus, the rate may not be asymptotically nonzero, as opposed to the case where we set $q = 2$.

Second and lastly, as discussed at the end of Section 2.5, it might be the case that restricting the set of lines forming recovery sets to those with high enough intersection number can yield sporadic good monomials in the same way as in the Hermitian-lifted code. The following conjecture focuses specifically on norm-trace-lifted codes with $q = 2$ but might be modified to capture a more general case. We state the norm-trace-lifted-specific version here because we have the exact intersection numbers for lines with these curves.

Conjecture 2.39. *For norm-trace-lifted codes with* $q = 2$*, if the set of recovery sets consists only of the non-tangent lines with intersection cardinality of* $2^{r-1} + 1$ *(so we discarded lines with intersection* $2^{r-1} - 1$*), then there are sporadic good monomials in the basis for the set of evaluation functions.*

Chapter 3

Fractional decoding of curve-lifted codes

Chapter 2 focused on recovery of erasures by accessing less information than usually is required. Fractional decoding techniques, introduced in [30], also facilitate error correction by downloading less received data than classical decoding algorithms. These methods are applicable in areas where data is stored, and has the possibility of corruption during storage. Additionally, instead of retrieving data from a proper subset of received symbols, algebraic properties of the field trace are employed to download only some λ-proportion of the received data (where $\lambda < 1$).

In Section 3.1, the procedure for fractional decoding of Reed-Solomon codes is summarized. Section 3.2 contains collaborative work with Gretchen L. Matthews and Welington Santos on fractional decoding of codes from the Hermitian curve. These results are extended to codes from the more general norm-trace curves in the same section. An improvement on these procedures involving use of alternate lines for recovery is laid out in Section 3.3, and is applied to codes from Hermitian curves, while also motivating application to Hermitian-lifted codes. The application to Hermitian-lifted codes is found in Section 3.4, and an analagous result for norm-trace-lifted codes is contained in Section 3.5. Future research directions and conjectures related to this work are outlined Section 3.6.

3.1 Preliminaries

We first set some notation. For $n \in \mathbb{Z}^+$, recall $[n] = \{1, \ldots, n\}$; we set $\underline{[n]} = \{0, \ldots, n-1\}$.

Consider the field extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$, and recall that the field trace of $\alpha \in \mathbb{F}_{q^2}$ with respect to this extension is

$$\mathrm{Tr}_{\mathbb{F}_{q^\ell}/\mathbb{F}_q}(\alpha) = \sum_{i=0}^{\ell-1} \alpha^{q^i} \in \mathbb{F}_q.$$

Remark 3.1. [16, Definition 2.30] Let $\mathcal{B} = \{\zeta_0, \ldots, \zeta_{\ell-1}\}$ be a basis for the extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$, and $\{\nu_0, \ldots, \nu_{\ell-1}\}$ be the corresponding dual basis of $\mathcal{B}$ with respect to the extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$. Then for each $\alpha \in \mathbb{F}_{q^\ell}$,

$$\alpha = \sum_{i=0}^{\ell-1} \mathrm{Tr}_{\mathbb{F}_{q^\ell}/\mathbb{F}_q}(\zeta_i \alpha)\nu_i.$$

Remark 3.2. Consider a polynomial

$$h(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{k-1}x^{k-1} \in \mathbb{F}_{q^\ell}[x]_{<k}.$$

For $i \in \underline{[\ell]}$, let

$$h_i(x) = \sum_{u=0}^{k-1} \mathrm{Tr}_{\mathbb{F}_{q^\ell}/\mathbb{F}_q}(\zeta_i \alpha_u)x^u \in \mathbb{F}_q[x]_{<k}.$$

Then $h(x)$ can be recovered from the set $\{h_i(x) : i \in \underline{[\ell]}\}$. Indeed,

$$\begin{aligned}
\sum_{i=0}^{\ell-1} \nu_i h_i(x) &= \sum_{i=0}^{\ell-1} \nu_i \left(\sum_{u=0}^{k-1} \mathrm{Tr}_{\mathbb{F}_{q^\ell}/\mathbb{F}_q}(\zeta_i \alpha_u)x^u \right) \\
&= \sum_{u=0}^{k-1} \left(\sum_{i=0}^{\ell-1} \mathrm{Tr}_{\mathbb{F}_{q^\ell}/\mathbb{F}_q}(\zeta_i \alpha_u)\nu_i \right) x^u \\
&= \sum_{u=0}^{k-1} \alpha_u x^u = h(x).
\end{aligned}$$

Remark 3.3. For $\alpha \in \mathbb{F}_{q^2}$, define

$$\Gamma_\alpha \coloneqq \{\beta \in \mathbb{F}_{q^2} : \beta^q + \beta = \alpha^{q+1}\}.$$

It is well-known that for all $\alpha \in \mathbb{F}_{q^2}$, $|\Gamma_\alpha| = q$. These sets partition the affine points on the Hermitian curve into q^2 distinct sets of q points; that is, if we denote for each $\alpha \in \mathbb{F}_{q^2}$ the set

$$P_\alpha \coloneqq \{(\alpha, \beta) : \beta \in \Gamma_\alpha\}$$

then

$$\mathcal{H}\left(\mathbb{F}_{q^2}\right) = \dot{\bigcup}_{\alpha \in \mathbb{F}_{q^2}} P_\alpha.$$

Fractional decoding of Reed-Solomon codes

We now proceed to review the fractional decoding procedure of a code over $\mathbb{F}_{q^\ell}$ introduced in [24]. Because the elements of the base field $\mathbb{F}_q$ can be expressed using fewer elements of $\mathbb{F}_q$ than elements of $\mathbb{F}_{q^\ell}$, we correct errors by downloading less information than is usually required. Specifically, for a code $C \subseteq \mathbb{F}_{q^\ell}^n$, a received word may be expressed using ℓn symbols of $\mathbb{F}_q$. Traditional decoding utilizes all ℓn symbols. Fractional decoding is a probabilistic algorithm which uses only $\lambda \ell n$ symbols of $\mathbb{F}_q$ where $\lambda < 1$. The procedure for fractional decoding of Reed-Solomon codes of Santos in [24] is presented first, since it inspired the fractional decoding for codes from the Hermitian curve.

Suppose $\Gamma \coloneqq \{\gamma_1, \ldots, \gamma_n\} \subseteq \mathbb{F}_q$, $\lambda = \frac{m}{\ell}$ where $m \in \mathbb{Z}^+$ such that $m < \ell$, $m|k$,

$$\{\gamma_1, \ldots, \gamma_k\} = A_0 \dot{\cup} \cdots \dot{\cup} A_{m-1} \subseteq \mathbb{F}_q$$

with $|A_j| = \frac{k}{m}$ for all $j \in \underline{[m]}$. For $j \in \underline{[m]}$, we set

$$p_j(x) \coloneqq \prod_{\alpha \in A_j} (x - \alpha) \in \mathbb{F}_q[x].$$

Then $p_j(a) = 0$ for all $\alpha \in A_j$, and $\deg p_j(x) = |A_j|$. For

$$h(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{k-1} x^{k-1} \in \mathbb{F}_{q^\ell}[x]_{<k}$$

and $j \in \underline{[m]}$, define

$$T_j(h)(x) = h_{\ell-m+j}(x)(p_j(x))^{(\ell-m)(j+1)} + \left[\sum_{u=0}^{\ell-m-1} h_u(x)(p_j(x))^{u(j+1)} \right] \in \mathbb{F}_q[x]_{<k_j}$$

where $k_j \coloneqq |A_j|(\ell - m)(j + 1) + k$.

Write

$$h(\Gamma) = (h(\alpha))_{\alpha \in \Gamma},$$

and

$$T_j(h)(\Gamma) = (T_j(h)(\alpha))_{\alpha \in \Gamma}.$$

Hence, for each $j \in \underline{[m]}$, see that

$$h(\Gamma) \in RS(q^\ell, n, k) \subseteq \mathbb{F}_{q^\ell}^n$$

which implies that

$$T_j(h)(\Gamma) \in RS(q, n, k_j) \subseteq \mathbb{F}_q^n.$$

Recalling that $|A_j| = \frac{k}{m}$ for all $j \in \underline{[m]}$, see that

$$k_0 < k_1 < \cdots < k_{m-1}.$$

We consider now the virtual projection of $C = RS(q^\ell, n, k)$ which is defined as the interleaved Reed-Solomon code [24]:

$$C_{P_{\frac{m}{\ell}}} = \left\{ \begin{bmatrix} T_0(h)(\Gamma) \\ T_1(h)(\Gamma) \\ \vdots \\ T_{m-1}(h)(\Gamma) \end{bmatrix} : h \in \mathbb{F}_{q^\ell}[x]_{<k} \right\} \subseteq \mathbb{F}_q^{m \times n}.$$

From here, we define the virtual projection of a received word $y \in \mathbb{F}_{q^\ell}^n$.

Definition 3.4. The *virtual projection* of $y \in \mathbb{F}_{q^\ell}^n$ is

$$\pi(y) \coloneqq \begin{bmatrix} d_1^0 & d_2^0 & \dots & d_n^0 \\ d_1^1 & d_2^1 & \dots & d_n^1 \\ \vdots & \vdots & & \vdots \\ d_1^{m-1} & d_2^{m-1} & \dots & d_n^{m-1} \end{bmatrix} \in \mathbb{F}_q^{m \times n}$$

where for each $i \in [n]$ and $j \in \underline{[m]}$,

$$d_i^j \coloneqq \mathrm{Tr}_{\mathbb{F}_{q^\ell}/\mathbb{F}_q}(\zeta_{\ell-m+j} y_i)(p_j(\gamma_i))^{(\ell-m)(j+1)} + \sum_{u=0}^{\ell-m-1} \mathrm{Tr}_{\mathbb{F}_{q^\ell}/\mathbb{F}_q}(\zeta_u y_i)(p_j(\gamma_i))^{u(j+1)} \in \mathbb{F}_q.$$

The virtual projection of a codeword $c \coloneqq ev(h) \in RS(q^\ell, n, k)$ may be viewed as a codeword

of an interleaved Reed-Solomon code,

$$\pi(c) \coloneqq \begin{bmatrix} T_0(h)(\Gamma) \\ T_1(h)(\Gamma) \\ \vdots \\ T_{m-1}(h)(\Gamma) \end{bmatrix} \in \mathbb{F}_q^{m \times n}.$$

These definitions are justified in the following lemma.

Lemma 3.5. *[24] Let $c \in RS(q^\ell, n, k)$ be a codeword. Assume that $y = c + e$ is a received word. If $e = (e_1, \ldots, e_n)$ has t nonzero coefficients $e_{i_1}, \ldots, e_{i_t}$ then the matrix $\pi(y)$ is a corrupted codeword of $C_{P_{\frac{m}{\ell}}}$ with at most t erroneous columns at the positions $i_1, \ldots, i_t$.*

Proof. If $e = 0$, then $y = c \in C$ is a codeword, then we know that $\pi(y)$ is a codeword of the virtual projection $C_{P_{\frac{m}{\ell}}}$. Note that

$$d_i^j = T_j(y)(\gamma_i) = T_j(c+e)(\gamma_i) = T_j(c)(\gamma_i) + T_j(e)(\gamma_i) = T_j(c)(\gamma_i).$$

Clearly, if $e_i = 0$, that is, if $i \notin \{i_1, \ldots, i_t\}$, then $T_j(e)(\gamma_i) = 0$ for all $j = 0, \ldots, m-1$. If $i \in \{i_1, \ldots, i_t\}$, then $T_j(e)(\gamma_i)$ may be nonzero, so Y has at most t erroneous columns. ■

The results of Santos in [24] use the collaborative decoding results of [25] for interleaved Reed-Solomon code. They provide a procedure for fractional decoding of Reed-Solomon codes, which we now describe.

For $j \in \underline{[m]}$ and $s \in \underline{[n - k_j]}$, let

$$S_{js} \coloneqq d_{k_j+s}^j.$$

For each $j \in \underline{[m]}$, define

$$S^{(j)} \coloneqq \begin{bmatrix} S_{j0} & \cdots & S_{jt-1} \\ S_{j1} & \cdots & S_{jt} \\ \vdots & & \vdots \\ S_{jn-k_j-t-1} & \cdots & S_{jn-k_j-2} \end{bmatrix} \in \mathbb{F}_q^{(n-k_j-t)\times t}$$

and

$$U^{(j)} \coloneqq \begin{bmatrix} -S_{jt} \\ -S_{jt+1} \\ \vdots \\ -S_{jn-k_j-1} \end{bmatrix} \in \mathbb{F}_q^{(n-k_j-t)\times 1}.$$

With these we set

$$S \coloneqq \begin{bmatrix} S^{(0)} \\ S^{(1)} \\ \vdots \\ S^{(m-1)} \end{bmatrix} \in \mathbb{F}_q^{\left(\sum_{j=0}^{m-1}(n-k_j-t)\right)\times t}$$

and

$$U \coloneqq \begin{bmatrix} U^{(0)} \\ U^{(1)} \\ \vdots \\ U^{(m-1)} \end{bmatrix} \in \mathbb{F}_q^{\left(\sum_{j=0}^{m-1}(n-k_j-t)\right)\times 1}.$$

The system we wish to solve is

$$S\Lambda = U,$$

which is a system of $\sum_{j=0}^{m-1}(n-k_j-t)$ equations in t unknowns $\Lambda_1,\ldots,\Lambda_t$, where

$$\Lambda \coloneqq \begin{bmatrix} \Lambda_t \\ \Lambda_{t-1} \\ \vdots \\ \Lambda_1 \end{bmatrix}.$$

Solving $S\Lambda = U$ produces an polynomial

$$E(x) = 1 + \sum_{i=1}^{t} \Lambda_i x^i,$$

called an error locator polynomial, as discussed in Definition 1.50. If $E(x)$ is separable over $\mathbb{F}_q$, we will see that t errors can be corrected; otherwise, the decoding is declared to be a failure. We describe this procedure in the following steps:

1. Download the mn entries of the virtual projection of $\pi(y) \in \mathbb{F}_q^{m\times n}$.

2. Determine the associated matrices S and U.

3. Solve the system $S\Lambda = U$ to determine the error locator polynomial $E(x)$.

4. If $E(x)$ is separable over $\mathbb{F}_q[x]$, determine c. Otherwise, declare decoding failure.

The separability of $E(x)$ gives the locations of the errors, which allows for decoding of received word y. Note that this procedure only required downloading $\lambda\ell n$ symbols of $\mathbb{F}_q$. Since $mn = \lambda\ell n$, this number of symbols is strictly less than the ℓn symbols that are normally required, since $\lambda < 1$. There is a limit on the number of errors that a code can correct with this procedure, called the λ-decoding radius.

Definition 3.6. For $\lambda \geq \frac{k}{n}$, we define the λ-decoding radius of C as the maximum number of errors that C can correct by downloading $\lambda n\ell$ symbols of $\mathbb{F}_q$, and denote it as τ_λ.

Given an $[n, k, d]$ linear code we should take $\lambda \geq \frac{k}{n}$, because a codeword encodes k data symbols. The decoder needs at least as many input symbols to decode the received word, even if no errors are present. If $\lambda = 1$, we return to the standard decoding problem. Thus, the goal of fractional decoding is study error correction for λ in the range $\frac{k}{n} \leq \lambda < 1$.

Proposition 3.7. *[24] Let $C = RS(q^\ell, n, k)$ be a Reed-Solomon code. Then its virtual projection code $C_{P_{\frac{m}{\ell}}}(q, n, \mathcal{K})$ attains the maximum possible decoding radius*

$$\tau_{P_{\frac{m}{\ell}}} = \frac{m}{m+2}\left(n - k - \frac{(\ell - m)}{m}\sum_{j=0}^{m-1}|A_j|(j+1)\right).$$

3.2 Fractional decoding of codes from the Hermitian curve

Previously, we saw that Reed-Solomon codes achieve the optimal λ-decoding radius for fractional decoding schemes. Though these codes are maximal, extending fractional decoding procedures to other classes of codes may allow us to utilize the desirable properties of those codes. Specifically, considering fractional decoding techniques applied to codes from the Hermitian curve, the desirable locality of these codes allows for more opportunities for decoding, which we will see in Section 3.3.

We now describe the procedure in [20] for fractional decoding of codes from the Hermitian curve. The inspiration for applying fractional decoding to codes from the Hermitian curve is that on each set $\mathcal{X}_q \cap \{x = \alpha\}$, we may perform Reed-Solomon fractional decoding. Throughout the rest of this section, because the Hermitian curve $\mathcal{X}_q$ is maximal over $\mathbb{F}_{q^2}$, we

consider the extension $\mathbb{F}_{q^{2\ell}}/\mathbb{F}_{q^2}$.

In the Reed-Solomon case, for any extension size ℓ, evaluation points with coordinates in $\mathbb{F}_q$ for the Reed-Solomon code are also evaluation points with coordinates in the extension field $\mathbb{F}_{q^\ell}$, since $\mathbb{F}_q \subseteq \mathbb{F}_{q^\ell}$, that is, points on the projective line over $\mathbb{F}_q$ may be considered points on the projective line over $\mathbb{F}_{q^\ell}$. However, it is not immediately clear that for the Hermitian curve over $\mathbb{F}_{q^2}$ that all its points are $\mathcal{X}_q(\mathbb{F}_{q^2}) \subseteq \mathcal{X}_{q^\ell}(\mathbb{F}_{q^{2\ell}})$, that is, it is not clear that the affine points on the Hermitian curve over $\mathbb{F}_{q^2}$ are affine points on the Hermitian curve over $\mathbb{F}_{q^{2\ell}}$.

Lemma 3.8. *Let $\mathcal{X}_{q^\ell} : x^{q^\ell+1} = y^{q^\ell} + y$ be the Hermitian curve over $\mathbb{F}_{q^{2\ell}}$ and $\mathcal{X}_q : x^{q+1} = y^q + y$ be the Hermitian curve over $\mathbb{F}_{q^2}$. If ℓ is odd, the all affine points of $\mathcal{X}_q$ with coordinates in $\mathbb{F}_{q^2}$ are precisely the affine points of $\mathcal{X}_{q^\ell}$ with coordinates in $\mathbb{F}_{q^2}$.*

Proof. Let $(a, b) \in \mathbb{F}_{q^2}^2$ be an affine point of $\mathcal{X}_q$. It is the case that $a^{q^2} = a$ and $b^{q^2} = b$, as $\mathbb{F}_{q^2}\backslash\{0\}$ is a cyclic group of order $q^2 - 1$ under multiplication. Note that since ℓ is odd $b^{q^\ell} = b^q$ and $a^{q^\ell+1} = a^{q+1}$. Therefore,

$$a^{q^\ell+1} = b^{q^\ell} + b$$

if and only if

$$a^{q+1} = b^q + b$$

proving that $\mathcal{X}_{q^\ell}(\mathbb{F}_{q^2}) = \mathcal{X}_q(\mathbb{F}_{q^2})$. ■

Now we detail the fractional decoding procedure. Let $f \in \mathcal{L}(MP_\infty) \subseteq \mathbb{F}_{q^{2\ell}}(\mathcal{X}_q)$ such that

there exist α_{ij} so that

$$f(x,y) = \sum_{j=0}^{R-1} \sum_{i=0}^{\lfloor \frac{M-j(q+1)}{q} \rfloor} \alpha_{ij} x^i y^j \in \mathbb{F}_{q^{2\ell}}[x,y]$$

for some $R < q$. For $\alpha \in \mathbb{F}_{q^2}$, let

$${}_\alpha f \coloneqq f(\alpha, y) \in \mathbb{F}_{q^{2\ell}}[y]_{<R}.$$

Denote the set of functions in $\mathcal{L}(MP_\infty)$ with degree in y strictly less than R by

$$\mathcal{L}_{R<q}(MP_\infty) \coloneqq \left\{ f(x,y) = \sum_{j=0}^{R-1} \sum_{i=0}^{\lfloor \frac{M-j(q+1)}{q} \rfloor} \alpha_{ij} x^i y^j : R < q, \alpha_{ij} \in \mathbb{F}_{q^{2\ell}} \right\} \subseteq \mathbb{F}_{q^{2\ell}}[x,y].$$

Thus, we write the code from the Hermitian curve as

$$C_{\mathcal{L}_{R<q}}(D, MP_\infty) = \left\{ (f(P_1), \ldots, f(P_{q^2}) : f \in \mathcal{L}_{R<q}(MP_\infty) \right\}.$$

We now set an enumeration of the elements of $\mathbb{F}_{q^2} = \{\alpha_1, \ldots, \alpha_{q^2}\}$ for the remainder of this development, so that the evaluation points of $C_{\mathcal{L}_{R<q}}(D, MP_\infty)$ are

$$(P_1, \ldots, P_n) = \left((P_{\alpha_i, \beta})_{\beta \in \Gamma_{\alpha_i}} \right)_{i=1}^{q^2}.$$

We may view a codeword as

$$ev(f) = \left({}_{\alpha_1} f(\Gamma_{\alpha_1}), {}_{\alpha_2} f(\Gamma_{\alpha_2}), \ldots, {}_{\alpha_{q^2}} f(\Gamma_{\alpha_{q^2}}) \right),$$

where for each $i \in [q^2]$

$$_{\alpha_i}f(\Gamma_{\alpha_i}) \coloneqq (_{\alpha_i}f(\beta))_{\beta \in \Gamma_{\alpha_i}}.$$

Notice that for $i \in [q^2]$ that

$$_{\alpha_i}f(\Gamma_{\alpha_i}) \in RS(q^{2\ell}, q, R).$$

The requirement $R < q$ guarantees that the minimum distance d of $RS(q^{2\ell}, q, R)$ satisfies $d \geq 2$ by the Singleton bound.

We now proceed to develop analagous objects to those in Section 3.1, taking into account the higher genus curve. Define subsets $A_{ij} \subseteq \mathbb{F}_{q^2}$ such that

$$\Gamma_{\alpha_i} \subseteq \bigcup_{j=0}^{\bullet\, m-1} A_{ij} \subseteq \mathbb{F}_{q^2}.$$

For $i \in [q^2]$ and $j \in \underline{[m]}$, set

$$p_{ij}(y) \coloneqq \prod_{\beta \in A_{ij}} (y - \beta)$$

and

$$T_{i,j}(f)(y) \coloneqq {}_{\alpha_i}f_{\ell-m+j}(y)(p_{ij}(y))^{(\ell-m)(j+1)} + \sum_{u=0}^{\ell-m-1} {}_{\alpha_i}f_u(y)(p_{ij}(y))^{u(j+1)}$$

where for $u \in \underline{[m]}$, the function ${}_{\alpha_i}f_u$ is defined to be

$${}_{\alpha_i}f_u(y) = \sum_{u=0}^{k_{ij}-1} \mathrm{Tr}_{\mathbb{F}_{q^{2\ell}}/\mathbb{F}_{q^2}}(\zeta_i \alpha_u) x^u \in \mathbb{F}_{q^2}[x]_{<k_{ij}}$$

and

$$k_{ij} \coloneqq |A_{ij}|(\ell - m)(j+1) + R$$

for all $i \in [q^2]$ and $j \in \underline{[m]}$. Then $T_{i,j}(f)(\Gamma_{\alpha_i}) \in RS(q^2, q, k_{ij})$. We now define the virtual projection of a function $f \in \mathcal{L}_{R<q}(MP_\infty)$.

Definition 3.9. Suppose $f \in \mathcal{L}_{R<q}(MP_\infty)$. The *virtual projection* of f is the matrix

$$\rho(f) \coloneqq \begin{bmatrix} T_{1,0}(f)(\Gamma_{\alpha_1}) & \cdots & T_{q^2,0}(f)(\Gamma_{\alpha_{q^2}}) \\ T_{1,1}(f)(\Gamma_{\alpha_1}) & \cdots & T_{q^2,1}(f)(\Gamma_{\alpha_{q^2}}) \\ \vdots & & \vdots \\ T_{1,m-1}(f)(\Gamma_{\alpha_1}) & \cdots & T_{q^2,m-1}(f)(\Gamma_{\alpha_{q^2}}) \end{bmatrix} \in \mathbb{F}_{q^2}^{m \times n}.$$

Note that for each $i \in [q^2]$ that ${}_{\alpha_i}f$ can be recovered from $\rho(f)$, since

$$\rho(f) \mid_{\Gamma_{\alpha_i}} = \begin{bmatrix} T_{i,0}(f)(\Gamma_{\alpha_i}) \\ T_{i,1}(f)(\Gamma_{\alpha_i}) \\ \vdots \\ T_{i,m-1}(f)(\Gamma_{\alpha_i}) \end{bmatrix} \in \mathbb{F}_{q^2}^{m \times q}$$

contains the only information needed for recovery of ${}_{\alpha_i}f$, since $\rho(f) \mid_{\Gamma_{\alpha_i}}$ is the virtual projection of the codeword

$$ev({}_{\alpha_i}f) = {}_{\alpha_i}f(\Gamma_{\alpha_i}) \in RS(q^{2\ell}, q, R).$$

Thus, we are able to use the Reed-Solomon fractional decoding procedure from [24] to recover each ${}_{\alpha_i}f$ assuming not too many errors have occurred.

We now proceed to describe recovering f from each ${}_{\alpha_i}f$. The number of terms of f is at most

$$\sum_{j=0}^{R-1} \sum_{i=0}^{\lfloor \frac{M-j(q+1)}{q} \rfloor} 1 \leq \lambda q^3 + q - \frac{q+1}{q} \sum_{i=0}^{q-1} i = \lambda q^3 + q - \frac{q^2}{2} < \lambda q^3 < q^3.$$

We then determine q^3 interpolation points, as $f(\alpha_i, \beta) = {}_{\alpha_i}f(\beta) \in \mathbb{F}_{q^{2\ell}}$ for all $\beta \in \Gamma_{\alpha_i}$. Thus, f can be recovered from ${}_{\alpha_i}f(y)$ for $i \in [q^2]$, unless too many errors have occurred.

Lastly, we define the virtual projection of a received word $y \in \mathbb{F}_{q^{2\ell}}^n$. For $i \in [q^2]$ write

$$\Gamma_{\alpha_i} = \{\beta_{i1}, \ldots, \beta_{iq}\} \subseteq \mathbb{F}_{q^2}.$$

For $i \in [q^2]$, $j \in [m]$, and $s \in [q]$, set

$$d_{is}^j \coloneqq \mathrm{Tr}_{\mathbb{F}_{q^{2\ell}}/\mathbb{F}_{q^2}}(\zeta_{\ell-m+j} y_i)(p_{ij}(\beta_{is}))^{(\ell-m)(j+1)} + \sum_{u=0}^{\ell-m-1} \mathrm{Tr}_{\mathbb{F}_{q^{2\ell}}/\mathbb{F}_{q^2}}(\zeta_u y_u)(p_{ij}(\beta_{is}))^{u(j+1)} \in \mathbb{F}_{q^2}.$$

Definition 3.10. The *virtual projection* of $y \in \mathbb{F}_{q^{2\ell}}^n$ is

$$\pi(y) \coloneqq \left[D_1 \mid \cdots \mid D_{q^2} \right] \in \mathbb{F}_{q^2}^{m \times n}$$

where

$$D_i = \begin{bmatrix} d_{i1}^0 & d_{i2}^0 & \ldots & d_{iq}^0 \\ d_{i1}^1 & d_{i2}^1 & \ldots & d_{iq}^1 \\ \vdots & \vdots & & \vdots \\ d_{i1}^{m-1} & d_{i2}^{m-1} & \ldots & d_{iq}^{m-1} \end{bmatrix} \in \mathbb{F}_{q^2}^{m \times q}$$

for all $i \in [q^2]$.

To see that $\pi(ev(f)) = \rho(f)$, see that Lemma 3.5 applies to each Reed-Solomon component $rho(f)|_{\Gamma_{\alpha_i}}$. Notice that the virtual projection of y contains $mn = \lambda \ell n$ entries of $\mathbb{F}_{q^2}$, as opposed to the usual ℓn entries of $\mathbb{F}_{q^2}$ that is normally used in decoding. We proceed to describe the fractional decoding algorithm, Algorithm 1. Suppose $y \in C_{\mathcal{L}_{R<q}}(D, MP_\infty)$ is a received word.

We declare decoding failure if for some $i \in [q^2]$, ${}_{\alpha_i}f$ fails to be recovered with Reed-Solomon decoding procedures. Thus for the Hermitian codeword to be recovered using Algorithm 1, all q^2 Reed-Solomon procedures must be successful. This means that if too many errors are

Algorithm 1 Virtual projection of codes from the Hermitian curve IRS decoder

Input: Received word $y = ev(f) + e$ where $f \in \mathcal{L}_{R<q}(MP_\infty)$, $\lambda = m/\ell$, and ℓ odd.
for $i \in [q^2]$ and $j \in \underline{[m]}$ **do**
  Download the entries of the virtual projection $\pi(y) \in \mathbb{F}_{q^2}^{m \times n}$.
  For each sub-matrix D_i of $\pi(y)$, perform the decoding procedure for Reed-Solomon codes described in Section 3.1 to recover ${}_{\alpha_i}f$.
  if ${}_{\alpha_i}f$ is recovered for each $i \in [q^2]$ **then**
    for each $s \in [q]$ **do**
      Calculate the points $(\alpha_i, {}_{\alpha_i}f(\beta_{is}))$.
      Use the results of the previous step to recover $f \in \mathcal{L}_{R<q}(MP_\infty)$.
    end for
  else
    Declare decoding failure.
  end if
end for
Output: $f \in \mathcal{L}_{R<q}(MP_\infty)$ or a decoding failure.

concentrated in any Γ_{α_i}, the entire codeword will fail to be recovered. Indeed, observe that we can correct t errors with

$$\min\left\{\tau_{\alpha_1}, \ldots, \tau_{\alpha_{q^2}}\right\} \leq t \leq \tau_{\alpha_1} + \cdots + \tau_{\alpha_{q^2}},$$

where τ_{α_i} is the decoding radius of the Reed-Solomon code yielding submatrix D_i. Improvements to the decoding radius of codes from the Hermitian curve will be addressed in Section 3.3.

Fractional decoding of codes from norm-trace curves

The procedure for fractional decoding of codes from the Hermitian curve used Remark 3.3 to form sets Γ_α which were of equal size. Each of these is a case where the Reed-Solomon fractional decoding procedure may be applied. This property of the field trace to partition the evaluation points from the Hermitian curve is present in other classes of algebraic curves

as well, such as the norm-trace curves, or quotients of function fields coming from either the Hermitian curve or norm-trace curves, which were introduced in Section 2.2.

Since norm-trace curves are defined over $\mathbb{F}_{q^r}$ and have q^{2r-1} affine points, we consider sets

$$\Gamma_\alpha = \left\{ \beta \in \mathbb{F}_{q^r} : \beta^{q^{r-1}} + \cdots + \beta^q + \beta = \alpha^{\frac{q^r-1}{q-1}} \right\}$$

each of which has size q^{r-1}. There are q^r of them, one corresponding to each $\alpha \in \mathbb{F}_{q^r}$.

An analog to Algorithm 1 consists of q^r Reed-Solomon fractional decoding procedures on $RS(q^{r\ell}, q^{r-1}, R)$ for some $R < q^{r-1}$.

As in the Hermitian case, where $\mathcal{X}_q(\mathbb{F}_{q^2}) \subseteq \mathcal{X}_{q^\ell}(\mathbb{F}_{q^{2\ell}})$ by Lemma 3.8, we show for norm-trace curves that $\mathcal{X}_{q,r}(\mathbb{F}_{q^r}) \subseteq \mathcal{X}_{q^\ell,r}(\mathbb{F}_{q^{2\ell}})$. Note that the condition in Lemma 3.11 was formulated in collaboration with Gretchen L. Matthews and Welington Santos, though the other discussion on fractional decoding of codes from norm-trace curves was developed independently.

Lemma 3.11. *Let $\mathcal{X}_{q^\ell,r} : x^{\frac{q^{r\ell}-1}{q^\ell-1}} = y^{q^{\ell(r-1)}} + \cdots + y^{q^\ell} + y$ be the norm-trace curve over $\mathbb{F}_{q^{r\ell}}$ and $\mathcal{X}_{q,r} : x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + \cdots + y^q + y$ be the norm-trace curve over $\mathbb{F}_{q^r}$. If $\ell \equiv 1$ mod r, the affine points of $\mathcal{X}_{q,r}$ with coordinates in $\mathbb{F}_{q^r}$ are precisely the affine points of $\mathcal{X}_{q^\ell,r}$ with coordinates in $\mathbb{F}_{q^r}$.*

Proof. Let $(a, b) \in \mathbb{F}_{q^r}^2$ be an affine point of $\mathcal{X}_{q,r}$. It is well-known that $a^{q^r} = a$ and $b^{q^r} = b$. Note since $\ell \equiv 1 \bmod r$, that the following holds for all $b \in \mathbb{F}_{q^r}$:

$$b^{q^{\ell(r-1)}} = b^{q^{\ell r-\ell}} = b^{q^r \cdot q^{(\ell-1)r-\ell}} = \left(b^{q^r}\right)^{q^{(\ell-1)r-\ell}} = b^{q^{(\ell-1)r-\ell}} = \cdots = b^{q^{(t+1)r-rt-1}} = b^{q^{r-1}}.$$

Therefore,

$$a^{\frac{q^{r\ell}-1}{q^\ell-1}} = b^{q^{\ell(r-1)}} + \cdots + b^{q^\ell} + b,$$

if and only if

$$a^{\frac{q^r-1}{q-1}} = b^{q^{r-1}} + \cdots + b^q + b$$

proving that $\mathcal{X}_{q^\ell,r}(\mathbb{F}_{q^r}) = \mathcal{X}_{q,r}(\mathbb{F}_{q^r})$. ■

Lemma 3.11 means that there exists at least q^{2r-1} affine points of $\mathcal{X}_{q^\ell,r}$ in $\mathbb{F}_{q^r}$ when $\ell \equiv 1 \bmod r$. In the following text, we only consider the case when $\ell \equiv 1 \bmod r$.

The procedure of fractional decoding for codes from norm-trace curves is inspired by that for Hermitian curves described in Section 3.2. We consider sets

$$\Gamma_\alpha = \left\{ \beta \in \mathbb{F}_{q^r} : \beta^{q^{r-1}} + \cdots + \beta^q + \beta = \alpha^{\frac{q^r-1}{q-1}} \right\}$$

where $\alpha \in \mathbb{F}_{q^r}$ and consider the extension $\mathbb{F}_{q^{r\ell}}/\mathbb{F}_{q^r}$.

Recall that on the norm-trace curve over $\mathbb{F}_{q^r}$, $x^i y^j \in \mathcal{L}(MP_\infty) \subseteq \mathbb{F}_{q^r}(\mathcal{X}_{q,r})$ if and only if

$$iq^{r-1} + j\left(\frac{q^r-1}{q-1}\right) \leq M.$$

Consider $f \in \mathcal{L}(MP_\infty) \subseteq \mathbb{F}_{q^{r\ell}}(\mathcal{X}_{q^\ell,r})$ such that there exist α_{ij} so that

$$f(x,y) = \sum_{j=0}^{R-1}\sum_{i=0}^{N} \alpha_{ij} x^i y^j \in \mathbb{F}_{q^{r\ell}}[x,y]$$

for some $R < q^{r-1}$, where

$$N = \left\lfloor \frac{M - j\left(\frac{q^r-1}{q-1}\right)}{q^{r-1}} \right\rfloor.$$

For $\alpha \in \mathbb{F}_{q^r}$, let

$${}_\alpha f \coloneqq f(\alpha, y) \in \mathbb{F}_{q^{r\ell}}[y]_{<R}.$$

Set

$$\mathcal{L}_{R<q^{r-1}}(MP_\infty) \coloneqq \left\{ f(x,y) = \sum_{j=0}^{R-1}\sum_{i=0}^{N} \alpha_{ij} x^i y^j : R < q^{r-1}, \alpha_{ij} \in \mathbb{F}_{q^{r\ell}} \right\} \subseteq \mathbb{F}_{q^{r\ell}}[x,y].$$

We must set an enumeration of the elements of $\mathbb{F}_{q^r} = \{\alpha_1, \ldots, \alpha_{q^r}\}$ for the remainder of this development, so that the evaluation points of $C_{\mathcal{L}_{R<q^{r-1}}}(D, MP_\infty)$ are

$$(P_1, \ldots, P_n) = \left((P_{\alpha_i,\beta})_{\beta \in \Gamma_{\alpha_i}} \right)_{i=1}^{q^r}.$$

Thus, we write the code from the norm-trace curve as

$$C_{\mathcal{L}_{R<q^{r-1}}}(D, MP_\infty) = \left\{ (f(P_1), \ldots, f(P_{q^r}) : f \in \mathcal{L}_{R<q^{r-1}}(MP_\infty) \right\}.$$

Write the codeword as

$$ev(f) = \left({}_{\alpha_1} f(\Gamma_{\alpha_1}), {}_{\alpha_2} f(\Gamma_{\alpha_2}), \ldots, {}_{\alpha_{q^r}} f(\Gamma_{\alpha_{q^r}}) \right).$$

Notice that for $i \in [q^r]$

$${}_{\alpha_i} f(\Gamma_{\alpha_i}) \in RS(q^{r\ell}, q^{r-1}, R).$$

We develop objects analagous to those Section 3.1, taking into account the higher genus curve. Define subsets $A_{ij} \subseteq \mathbb{F}_{q^r}$ such that

$$\Gamma_{\alpha_i} \subseteq \bigcupdot_{j=0}^{m-1} A_{ij} \subseteq \mathbb{F}_{q^r}.$$

For $i \in [q^r]$ and $j \in \underline{[m]}$, set

$$p_{ij}(y) \coloneqq \prod_{\beta \in A_{ij}} (y - \beta)$$

and

$$T_{i,j}(f)(y) \coloneqq {}_{\alpha_i}f_{\ell-m+j}(y)(p_{ij}(y))^{(\ell-m)(j+1)} + \sum_{u=0}^{\ell-m-1} {}_{\alpha_i}f_u(y)(p_{ij}(y))^{u(j+1)}$$

where for $u \in \underline{[m]}$, the function ${}_{\alpha_i}f_u$ is defined to be

$${}_{\alpha_i}f_u(y) = \sum_{u=0}^{k_{ij}-1} \mathrm{Tr}_{\mathbb{F}_{q^{r\ell}}/\mathbb{F}_{q^r}}(\zeta_i\alpha_u)x^u \in \mathbb{F}_{q^r}[x]_{<k_{ij}}$$

and

$$k_{ij} \coloneqq |A_{ij}|(\ell-m)(j+1) + R$$

for all $i \in [q^r]$ and $j \in \underline{[m]}$. Then $T_{i,j}(f)(\Gamma_{\alpha_i}) \in RS(q^r, q^{r-1}, k_{ij})$. We now define the virtual projection of a function $f \in \mathcal{L}_{R<q^{r-1}}(MP_\infty)$.

Definition 3.12. Suppose $f \in \mathcal{L}_{R<q^{r-1}}(MP_\infty)$. The *virtual projection* of f is the matrix

$$\rho(f) \coloneqq \begin{bmatrix} T_{1,0}(f)(\Gamma_{\alpha_1}) & \cdots & T_{q^r,0}(f)(\Gamma_{\alpha_{q^r}}) \\ T_{1,1}(f)(\Gamma_{\alpha_1}) & \cdots & T_{q^r,1}(f)(\Gamma_{\alpha_{q^r}}) \\ \vdots & & \vdots \\ T_{1,m-1}(f)(\Gamma_{\alpha_1}) & \cdots & T_{q^r,m-1}(f)(\Gamma_{\alpha_{q^r}}) \end{bmatrix} \in \mathbb{F}_{q^r}^{m\times n}.$$

Note that for each $i \in [q^r]$ that ${}_{\alpha_i}f$ can be recovered from $\rho(f)$, since

$$\rho(f)\mid_{\Gamma_{\alpha_i}} = \begin{bmatrix} T_{i,0}(f)(\Gamma_{\alpha_i}) \\ T_{i,1}(f)(\Gamma_{\alpha_i}) \\ \vdots \\ T_{i,m-1}(f)(\Gamma_{\alpha_i}) \end{bmatrix} \in \mathbb{F}_{q^r}^{m\times q^{r-1}}$$

contains the necessary information for recovery of ${}_{\alpha_i}f$, since $\rho(f)\mid_{\Gamma_{\alpha_i}}$ is the virtual projection

of the codeword

$$ev({}_{\alpha_i}f) = {}_{\alpha_i}f(\Gamma_{\alpha_i}) \in RS(q^{r\ell}, q^{r-1}, R).$$

Thus, we are able to use the Reed-Solomon fractional decoding procedure from [24] to recover each ${}_{\alpha_i}f$ assuming not too many errors have occurred.

We now proceed to describe recovering f from each ${}_{\alpha_i}f$. The number of terms of f is no more than q^{2r-1}. We then may determine q^{2r-1} interpolation points, as $f(\alpha_i, \beta) = {}_{\alpha_i}f(\beta) \in \mathbb{F}_{q^{r\ell}}$ for all $\beta \in \Gamma_{\alpha_i}$. Thus, f can be recovered from ${}_{\alpha_i}f(y)$ for $i \in [q^r]$, if not too many errors have occurred.

Lastly, we define the virtual projection of a received word $y \in \mathbb{F}_{q^{r\ell}}^n$. For $i \in [q^r]$, write

$$\Gamma_{\alpha_i} = \{\beta_{i1}, \ldots, \beta_{iq^{r-1}}\} \subseteq \mathbb{F}_{q^r}.$$

For $i \in [q^r]$, $j \in [m]$, and $s \in [q^{r-1}]$, set

$$d_{is}^j \coloneqq \mathrm{Tr}_{\mathbb{F}_{q^{r\ell}}/\mathbb{F}_{q^r}}(\zeta_{\ell-m+j} y_i)(p_{ij}(\beta_{is}))^{(\ell-m)(j+1)} + \sum_{u=0}^{\ell-m-1} \mathrm{Tr}_{\mathbb{F}_{q^{r\ell}}/\mathbb{F}_{q^r}}(\zeta_u y_u)(p_{ij}(\beta_{is}))^{u(j+1)} \in \mathbb{F}_{q^r}.$$

Definition 3.13. The *virtual projection* of $y \in \mathbb{F}_{q^{r\ell}}^n$ is

$$\pi(y) \coloneqq \left[D_1 \mid \cdots \mid D_{q^r} \right] \in \mathbb{F}_{q^r}^{m \times n}$$

where

$$D_i = \begin{bmatrix} d_{i1}^0 & d_{i2}^0 & \ldots & d_{iq^{r-1}}^0 \\ d_{i1}^1 & d_{i2}^1 & \ldots & d_{iq^{r-1}}^1 \\ \vdots & \vdots & & \vdots \\ d_{i1}^{m-1} & d_{i2}^{m-1} & \ldots & d_{iq^{r-1}}^{m-1} \end{bmatrix} \in \mathbb{F}_{q^r}^{m \times q^{r-1}}$$

for all $i \in [q^r]$.

To see that $\pi(ev(f)) = \rho(f)$, see that Lemma 3.5 applies to each Reed-Solomon component $rho(f)|_{\Gamma_{\alpha_i}}$. The virtual projection of y contains $mn = \lambda\ell n$ entries of $\mathbb{F}_{q^r}$, as opposed to the usual ℓn entries of $\mathbb{F}_{q^r}$. We proceed to describe the decoding algorithm, shown in Algorithm 2.

Algorithm 2 Virtual projection of codes from norm-trace curves IRS decoder

Input: Received word $y = ev(f) + e$ where $f \in \mathcal{L}_{R<q^{r-1}}(MP_\infty)$, $\lambda = m/\ell$, and $\ell \equiv 1 (\text{mod } r)$.
for $i \in [q^r]$ and $j \in \underline{[m]}$ **do**
  Download the entries of the virtual projection $\pi(y) \in \mathbb{F}_{q^r}^{m\times n}$.
  For each sub-matrix D_i of $\pi(y)$, perform the decoding procedure for Reed-Solomon codes described in Section 3.1 to recover ${}_{\alpha_i}f$.
  if ${}_{\alpha_i}f$ is recovered for each $i \in [q^r]$ **then**
    for each $s \in [q^{r-1}]$ **do**
      Calculate the points $(\alpha_i, {}_{\alpha_i}f(\beta_{is}))$.
      Use the results of the previous step to recover $f \in \mathcal{L}_{R<q^{r-1}}(MP_\infty)$.
    end for
  else
    Declare decoding failure.
  end if
end for
Output: $f \in \mathcal{L}_{R<q^{r-1}}(MP_\infty)$ or a decoding failure.

We declare decoding failure if for some $i \in [q^r]$, ${}_{\alpha_i}f$ fails to be recovered with Reed-Solomon decoding procedures.

3.3 Alternate recovery lines for the Hermitian case

As noted in Section 3.2, one weakness of the fractional decoding procedures for codes $C_{\mathcal{L}_{R<q}}(D, MP_\infty)$ from the Hermitian curve as it is presented in [20] is that, for the decoding of the codeword $c \in C_{\mathcal{L}_{R<q}}(D, MP_\infty)$ to be successful, the decoding for each Reed-Solomon piece $RS(q^{2\ell}, q, R)$ has to be successful. A failure declared for any of the sets Γ_{α_i} means declaring failure for the entire received word. Recall Remark 2.1, which stated that every

non-tangent line over $\mathbb{F}_{q^2}$ intersects the Hermitian curve in exactly $q+1$ places.

Notice that the sets Γ_{α_i} defined in [20] are vertical lines in the space $\mathbb{F}_{q^2}^2$; that is, sets of points (α, β) with the first coordinate α, for some $\alpha \in \mathbb{F}_{q^2}$. A failure of the fractional decoding procedure of [20] means that too many errors are contained in one vertical line Γ_α. However, this inability to correct one Reed-Solomon component does not mean that there are too many errors for the code to correct. Note that for vertical lines, since one place is the place at infinity, there are only q affine points of intersection; for other non-tangent lines, there are $q+1$ affine points of intersection.

Thus, we consider fractional decoding using lines other than vertical lines. If there are too many errors in one vertical set Γ_{α_i}, then considering other sets Γ formed from non-vertical lines may spread out the errors enough so that the errors may be corrected, by considering Reed-Solomon components $RS(q^{2\ell}, q+1, R)$. Such sets are compared to the standard vertical sets Γ_α in Figures 3.1 and 3.2, where Figure 3.1 represents the sets detailed in [20], and Figure 3.2 represents the new proposed lines for forming repair groups.

However, these sets of points are formed differently; in the original procedure, we restricted the power on y in the function f to be at most some $R < q$. This is the same as restricting to a low-degree polynomial in y on the relevant line $x = \alpha$, which is exactly the idea employed in the case of Hermitian-lifted codes $C_{\mathcal{X}_q}$, to only use polynomials which restrict to a low-enough degree univariate polynomial on the intersection of any non-tangent line with the Hermitian curve. Additionally, the basis for the space of evaluation polynomials for one-point Hermitian codes $C(D, MP_\infty)$ is contained in the basis $\mathcal{F}$ given for Hermitian-lifted codes $\mathcal{C}_{\mathcal{X}_q}$, and so all the evaluation polynomials $f(x,y) \in \mathcal{L}_{R<q}(MP_\infty)$ we have considered so far have the restriction property that desired here. In other words, the set of evaluation functions is all $f \in \mathcal{F}$ from Definition 2.2.

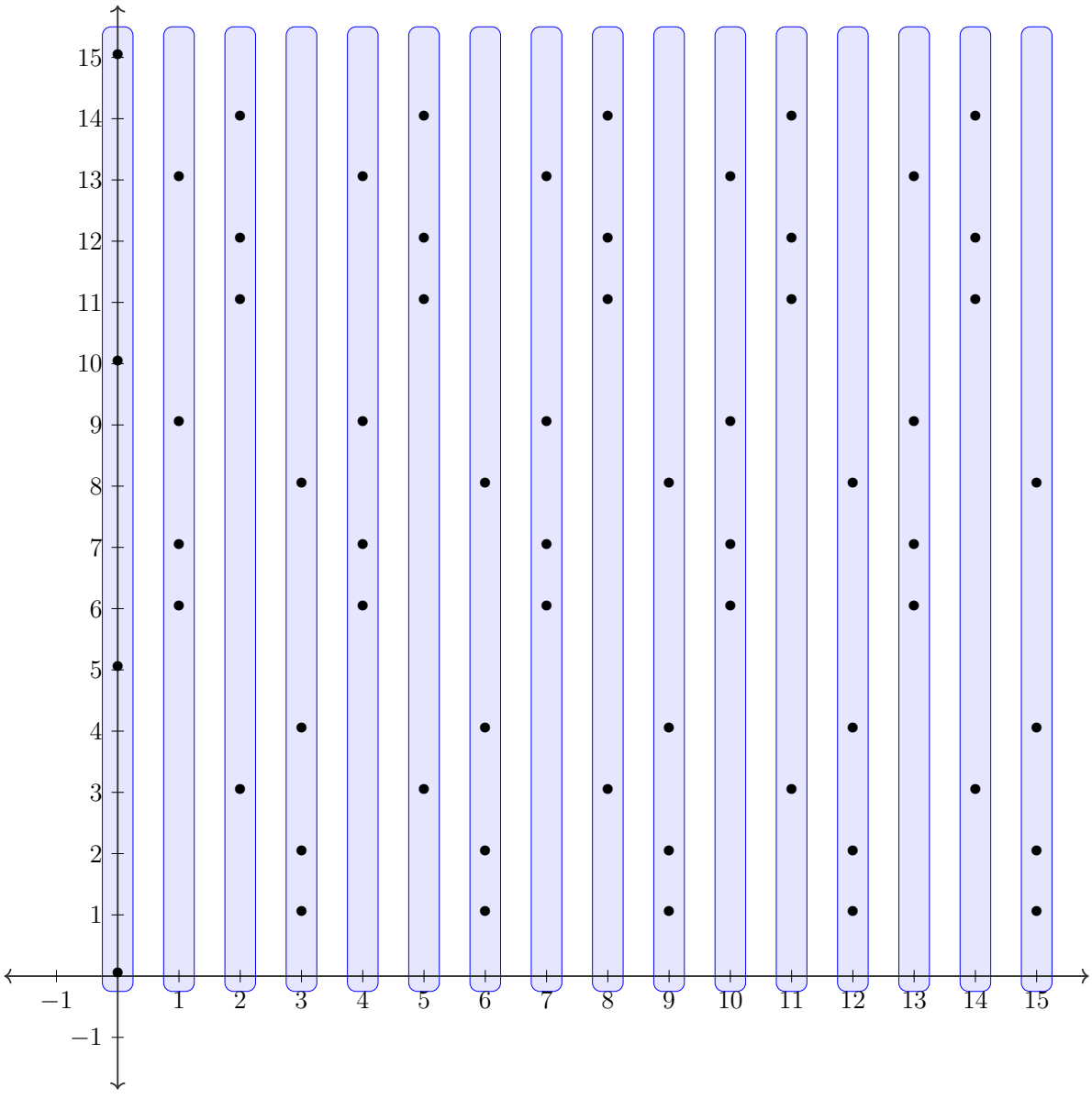

Figure 3.1: Partition of Hermitian points over $\mathbb{F}_{16}$ with vertical lines.

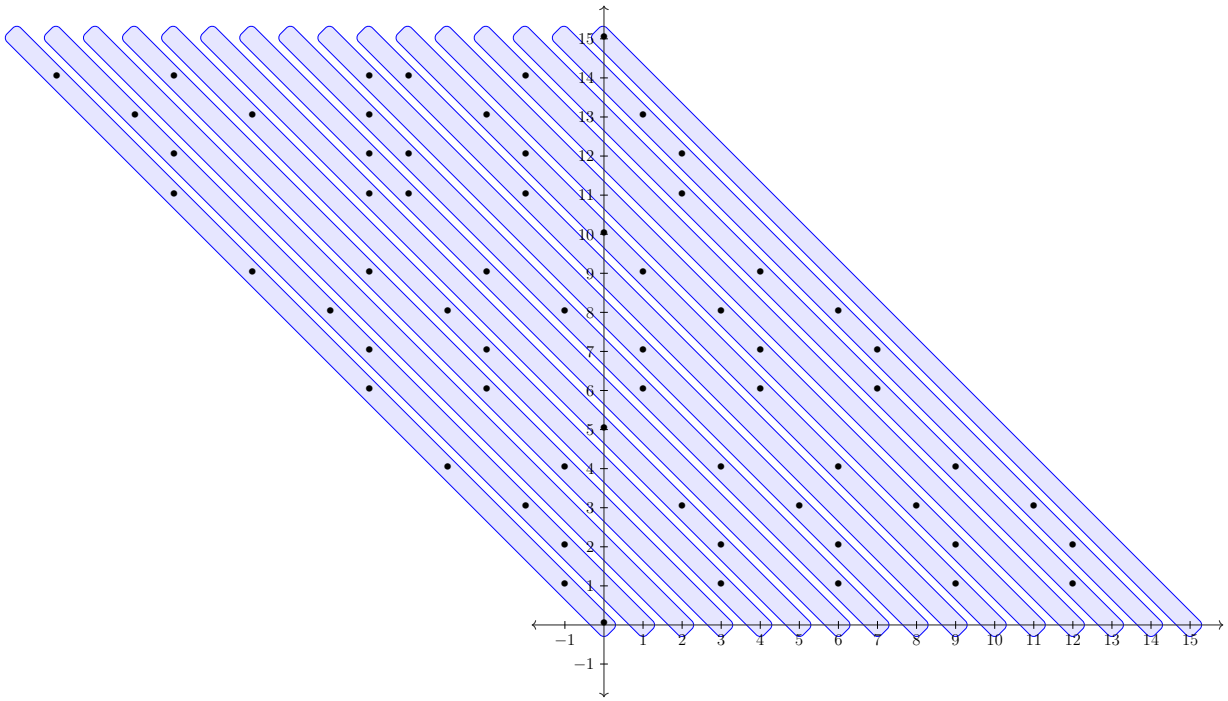

Figure 3.2: Idea of a partition of Hermitian points over $\mathbb{F}_{16}$ with non-vertical lines.

A new procedure incorporating this idea is to start with vertical lines. If failure is declared for any of the submatrices D_i of the virtual projection, re-start the procedure with an alternate set of parallel non-tangent lines. Non-vertical lines again partition the set of points, and have the capacity to spread out the errors among the lines enough for correction. Instead of forming sets

$$\Gamma_\alpha = \{\beta \in \mathbb{F}_{q^2} : \beta^q + \beta = \alpha^{q+1}\},$$

we need to parametrize the sets with two variables. Set a slope $0 \neq \hat{\alpha} \in \mathbb{F}_{q^2}$, and define Γ'_{β_i} by

$$\Gamma'_{\beta_i} \coloneqq \{(\alpha, \beta) \in \mathbb{F}_{q^2} : \beta = \hat{\alpha}\alpha + \beta_i, \beta^q + \beta = \alpha^{q+1}\}.$$

In the above definition, the first condition that $\beta = \hat{\alpha}\alpha + \beta_i$ guarantees the points in Γ'_{β_i} lie on the line formed by β_i with slope $\hat{\alpha}$, and the second guarantees the points in Γ'_{β_i} are on the Hermitian curve $x^{q+1} = y^q + y$ over $\mathbb{F}_{q^2}$. The q^2 values of $\beta_i \in \mathbb{F}_{q^2}$ form a partition $\{\Gamma'_{\beta_i}\}$

of the affine points on the Hermitian curve.

Since there are $q^2 - 1$ sets of non-horizontal lines, as there are $q^2 - 1$ non-zero slopes $\hat{\alpha}$ for lines in $\mathbb{F}_{q^2}^2$, this procedure allows for $q^2 - 2$ more opportunities to recover errors using non-vertical, non-horizontal lines to partition the space $\mathbb{F}_{q^2}^2$.

However, because non-vertical non-tangent lines intersect the Hermitian curve in $q+1$ affine points over $\mathbb{F}_{q^2}$, we do not get the partition into q^2 sets each of size q that we had when considering only vertical lines. Instead, if we set $\hat{\alpha}$ for the lines, then the set of lines with slope $\hat{\alpha}$ partition the affine points into $q^2 - q$ sets each of size $q+1$, and q sets of size 1. We then repair the $q^2 - q$ points partitioned by non-tangent lines, and if no failure occurs, then for the remaining q points consider all non-tangent lines through that point and perform the fractional decoding procedure.

While this procedure is likely not the most efficient structuring of such a fractional decoding algorithm for codes from the Hermitian curve with non-vertical lines, it does show that use of non-vertical lines is possible. The procedure is described and presented in Algorithm 3.

3.4 Fractional decoding of Hermitian-lifted codes

It was discussed in Section 3.3 that the restriction that the degree R in y of $f(x, y)$, namely that $R < q$, for the codes from the Hermitian curve is in effect restricting the monomials $x^i y^j$ in an evaluation function f to be of low enough degree over the vertical line given by $x = \alpha$ for some $\alpha \in \mathbb{F}_{q^2}$. This consideration is exactly the one made in defining good monomials in the Hermitian-lifted code construction.

A key observation here is that not only the monomials for the one-point Hermitian codes $C(D, MP_\infty)$ are included in the basis for the evaluation functions, but also the sporadic good

Algorithm 3 Virtual projection of codes from the Hermitian curve IRS decoder, non-vertical lines

Input: Received word $y = ev(f) + e$ where $f \in \mathcal{L}_{R<q}(MP_\infty)$ with $f \in \mathcal{F}$, $\lambda = m/\ell$, and ℓ odd.
Run Algorithm 1 for vertical lines
if f is recovered by Algorithm 1 **then**
  return $f \in \mathcal{L}_{R<q}(MP_\infty)$
else
  for $\hat{\alpha} \in \mathbb{F}_{q^2}$ with $\hat{\alpha} \neq 0$ **do**
    for $\beta_i \in \mathbb{F}_{q^2}$ **do**
      if $|\Gamma'_{\beta_i}| = q + 1$ **then**
        Download the entries of the virtual projection formed by the points of Γ'_{β_i}, and perform the decoding procedure for Reed-Solomon codes described in Section 3.1 to recover $f|_{\Gamma'_{\beta_i}}$.
      end if
    end for
    if all $q^2 - q$ functions $f|_{\Gamma'_{\beta_i}}$ were successfully recovered **then**
      for each of the q remaining affine points P **do**
        for all non-tangent lines L through P **do**
          Download the entries of the virtual projection formed by the points of $L \cap \mathcal{X}_q$ and perform the decoding procedure for Reed-Solomon codes described in Section 3.1 to recover $f|_{L\cap\mathcal{X}_q}$.
        end for
      end for
    else
      Break and iterate to a new $\hat{\alpha}$.
    end if
    if functions for each of the remaining q points were recovered successfully **then**
      Calculate evaluations of the relevant functions on each of the q^3 points.
      Use the results of the previous step to recover $f \in \mathcal{L}_{R<q}(MP_\infty) \cap \mathcal{F}$.
      return $f \in \mathcal{L}_{R<q}(MP_\infty) \cap \mathcal{F}$
    end if
  end for
  if f was not recovered during any iteration **then**
    Declare decoding failure.
  end if
end if
Output: $f \in \mathcal{L}_{R<q}(MP_\infty) \cap \mathcal{F}$ or a decoding failure.

monomials $x^i y^j \in \mathcal{F}$ which had $i+j > q$, where we recall that q is the locality for Hermitian-lifted codes $\mathcal{C}_{\mathcal{X}_q}$. To define a fractional decoding procedure for codes from Hermitian-lifted codes, notice that the space of evaluation functions f we may consider is larger than that for the codes from the Hermitian curve considered thus far. Therefore, instead of considering

$$f(x,y) = \sum_{j=0}^{R-1} \sum_{i=0}^{\lfloor \frac{M-j(q+1)}{q} \rfloor} \alpha_{ij} x^i y^j \in \mathbb{F}_q^{2\ell}[x,y]$$

we consider the broader class of functions

$$f(x,y) = \sum_{M_{i,j}(x,y) \in \mathcal{F}} \alpha_{ij} M_{i,j}(x,y) \in \mathbb{F}_q^{2\ell}[x,y].$$

Recall $\mathcal{F}$ from Definition 2.12 is the set of monomials which, when considered over intersections $\mathcal{X}_q \cap L_{\alpha,\beta}$, restrict to low-degree polynomials.

Additionally, because the set of evaluation functions is extended by considering the good monomials of the Hermitian-lifted code construction, the improvement discussed in Section 3.3 is naturally incorporated into this procedure. Indeed good monomials restrict to low enough degree polynomials on every non-horizontal line. The only change made to Algorithm 3 is that, because vertical lines only intersect the curve in q affine points, we do not use those for error correction. We are still able to use the procedure with the sets Γ'_{β_i} formed by non-tangent lines. This idea is presented in Algorithm 4.

3.5 Fractional decoding of norm-trace-lifted codes

Algorithm 4 in Section 3.2 extends naturally to norm-trace-lifted codes with $q = 2$. This is enabled by the intersection numbers $|L_{\alpha,\beta} \cap \mathcal{X}_{2,r}|$ of non-horizontal lines with the curve being

Algorithm 4 Virtual projection of Hermitian-lifted codes IRS decoder

Input: Received word $y = ev(f) + e$ where $f \in \mathcal{F}$, $\lambda = m/\ell$, and ℓ odd.
for $\hat{\alpha} \in \mathbb{F}_{q^2}$ with $\hat{\alpha} \neq 0$ **do**
  for $\beta_i \in \mathbb{F}_{q^2}$ **do**
    if $|\Gamma'_{\beta_i}| = q + 1$ **then**
      Download the entries of the virtual projection formed by the points of Γ'_{β_i}, and perform the decoding procedure for Reed-Solomon codes described in Section 3.1 to recover $f|_{\Gamma'_{\beta_i}}$.
    end if
  end for
  if all $q^2 - q$ functions $f|_{\Gamma'_{\beta_i}}$ were successfully recovered **then**
    for each of the q remaining affine points P **do**
      for all non-tangent lines L through P **do**
        Download the entries of the virtual projection formed by the points of $L \cap \mathcal{X}_q$ and perform the decoding procedure for Reed-Solomon codes described in Section 3.1 to recover $f|_{L \cap \mathcal{X}_q}$.
      end for
    end for
  else
    Break and iterate to a new $\hat{\alpha}$.
  end if
  if functions for each of the remaining q points were recovered successfully **then**
    Calculate evaluations of the relevant functions on each of the q^3 points.
    Use the results of the previous step to recover $f \in \mathcal{F}$.
    return $f \in \mathcal{F}$
  end if
end for
if f was not recovered during any iteration **then**
  Declare decoding failure.
end if
Output: $f \in \mathcal{F}$ or a decoding failure.

at least $2^{r-1}-1$ from Lemma 2.10.

By Lemmas 2.9 and 2.10, there all tangent lines have slope zero. However, because non-tangent lines do not all intersect the curve in the same number of places as the Hermitian curve does, the error correcting capacity of the Reed-Solomon blocks is restricted by the smallest intersection number of $2^{r-1}-1$. This bound is analagous to the locality in the case of the norm-trace-lifted codes. Additionally, as a result of the non-constant intersection numbers, the blocks D_i are of slightly different widths, either $2^{r-1}-1$ or $2^{r-1}+1$. No issue is presented however, as having $2^{r-1}+1$ evaluation points instead of $2^{r-1}-1$ does not decrease the effectiveness of fractional decoding of the Reed-Solomon block. Algorithm 5 describes this procedure.

Algorithm 5 Virtual projection of norm-trace-lifted codes IRS decoder

Input: Received word $y = ev(f) + e$ where $f \in \mathcal{F}$, $\lambda = m/\ell$, and $\ell \equiv 1 (\text{mod } r)$.
for $\hat{\alpha} \in \mathbb{F}_{2^r}$ with $\hat{\alpha} \neq 0$ **do**
  for $\beta_i \in \mathbb{F}_{2^r}$ **do**
    Download the entries of the virtual projection formed by the points of Γ'_{β_i}, and perform the decoding procedure for Reed-Solomon codes described in Section 3.1 to recover $f|_{\Gamma'_{\beta_i}}$.
  end for
  if all 2^r Reed-Solomon blocks are successfully decoded **then**
    Calculate evaluations of the relevant functions on each of the q^{2r-1} points.
    Use the results of the previous step to recover $f \in \mathcal{F}$.
    return $f \in \mathcal{F}$
  end if
end for
if f was not recovered during any iteration **then**
  Declare decoding failure.
end if
Output: $f \in \mathcal{F}$ or a decoding failure.

3.6 Future research

The fractional decoding procedure of [24] shows that Reed-Solomon codes achieve the optimal λ-decoding radius for fractional decoding procedures. One problem for future research is to determine the λ-decoding radius for these codes from Hermitian curves and norm-trace curves. Just as in the work of [20] on codes from the Hermitian curve, it is still an open problem to determine the exact λ-decoding radius for any of the codes discussed.

Another direction of research is to consider the fractional decoding of more general norm-trace-lifted codes. However, the same issue of not knowing the intersection number between lines and norm-trace curves is prohibitive. The family of Suzuki curves could yield interesting results, because of their space-filling nature, as every line over $\mathbb{F}_q$ intersects the Suzuki curve in q distinct affine points. However, there may be challenges generated by basis elements of $\mathcal{L}(mP_\infty)$ that are not polynomials. Beyond the Suzuki curve, there may be other curve-lifted codes that can be decoded in this fashion.

A final direction of research worth mentioning is using other interleaved codes from algebraic geometry codes, like the Hermitian code, and the collaborative decoding results that already exist for such codes [6, 22]. Although fractional decoding of codes from the Hermitian curve in the fashion of [20] suggests fractional decoding of Hermitian-lifted codes, it is still an interesting question to see if interleaved Hermitian codes can be utilized in these decoding procedures.

In further work, we may also consider approaches to prove the following conjecture related to norm-trace-lifted codes.

In Section 3.2, the procedure of fractional decoding of codes from the Hermitian curve was adapted to the more general norm-trace codes. Because this partitioning property is inherent to the field trace, not just to Hermitian curves or norm-trace curves, it could be that the

extension to the quotients defined in Section 2.2 is just as straightforward.

Conjecture 3.14. *The fractional decoding procedures laid out in Algorithms 1 and 2 apply similarly to curves from quotients of the Hermitian and norm-trace function fields.*

For the above conjecture, however, we need results analagous to those in Lemma 3.8 and Lemma 3.11.

The methods of fractional decoding applied to codes from both the Hermitian and norm-trace curves suggests there is much more work to be done applying fractional decoding techniques to codes from algebraic curves. This is an area of interest, since the locality and availability naturally offered by utilizing these algebraic curves is beneficial in data storage applications, where fractional decoding may also be applied. Additionally, the extension of fractional decoding to norm-trace-lifted codes may suggest an approach to fractional decoding of locally recoverable codes in general, as well as a bound on the decoding radius of codes with locality and availability.

Bibliography

[1] Edoardo Ballico and Chiara Marcolla. Higher Hamming weights for locally recoverable codes on algebraic curves. *Finite Fields and Their Applications*, 40:61–72, 2016.

[2] Alexander Barg, Itzhak Tamo, and Serge Vlăduţ. Locally recoverable codes on algebraic curves. *IEEE Transactions on Information Theory*, 63(8):4928–4939, 2017.

[3] Daniele Bartoli, Maria Montanucci, and Luciane Quoos. Locally recoverable codes from automorphism group of function fields of genus $g \geq 1$. *IEEE Transactions on Information Theory*, 66(11):6799–6808, 2020.

[4] Matteo Bonini and Massimiliano Sala. Intersections between the norm-trace curve and some low degree curves. *Finite Fields and Their Applications*, 67:101715, 2020.

[5] Matteo Bonini, Massimiliano Sala, and Lara Vicino. Rational points on cubic surfaces and AG codes from the norm-trace curve. *arXiv preprint arXiv:2102.05478*, 2021.

[6] Andrew Brown, Lorenz Minder, and Amin Shokrollahi. Probabilistic decoding of interleaved RS-codes on the q-ary symmetric channel. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, pages 326–326. IEEE, 2004.

[7] Jeanne Fitzgerald and Robert F Lax. Decoding affine variety codes using Gröbner bases. *Designs, Codes and Cryptography*, 13(2):147–158, 1998.

[8] Arnaldo Garcia. Curves over finite fields attaining the Hasse-Weil upper bound. In *European Congress of Mathematics*, pages 199–205. Springer, 2001.

[9] Olav Geil. On codes from norm-trace curves. *Finite Fields and their Applications*, 9(3):351 – 371, 2003.

[10] Parikshit Gopalan, Cheng Huang, Bob Jenkins, and Sergey Yekhanin. Explicit maximally recoverable codes with locality. *IEEE Transactions on Information Theory*, 60(9):5245–5256, 2014.

[11] Parikshit Gopalan, Cheng Huang, Huseyin Simitci, and Sergey Yekhanin. On the locality of codeword symbols. *IEEE Transactions on Information theory*, 58(11):6925–6934, 2012.

[12] Valerii Denisovich Goppa. Algebraico-geometric codes. *Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya*, 46(4):762–781, 1982.

[13] Venkatesan Guruswami, Atri Rudra, and Madhu Sudan. Essential coding theory. *Draft available at http://www. cse. buffalo. edu/ atri/courses/coding-theory/book*, 2012.

[14] Johan P Hansen and Henning Stichtenoth. Group codes on certain algebraic curves with many rational points. *Applicable Algebra in Engineering, Communication and Computing*, 1(1):67–77, 1990.

[15] James William Peter Hirschfeld, Gábor Korchmáros, Fernando Torres, and Fernando Eduardo Torres Orihuela. *Algebraic curves over a finite field*. Princeton University Press, 2008.

[16] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Cambridge University Press, Cambridge, Great Britain, 2^{nd} edition, 1997.

[17] Hedongliang Liu, Lukas Holzbaur, Nikita Polyanskii, Sven Puchinger, and Antonia Wachter-Zeh. Quadratic-curve-lifted Reed-Solomon codes. *arXiv preprint arXiv:2109.14478*, 2021.

[18] Hiram López, Beth Malmskog, Gretchen Matthews, Fernando Piñero-González, and

Mary Wootters. Hermitian-lifted codes. *Designs, Codes, and Cryptography*, 89:497 – 515, 2021.

[19] Gretchen L Matthews. Codes from the Suzuki function field. *IEEE Transactions on Information Theory*, 50(12):3298–3302, 2004.

[20] Gretchen L Matthews, Aidan W Murphy, and Welington Santos. Fractional decoding of codes from Hermitian curves. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 515–520. IEEE, 2021.

[21] C. Munuera, G.C. Tizziotti, and F. Torres. Two-point codes on norm-trace curves. In *Coding Theory and Applications*. Springer, September 2008.

[22] Sven Puchinger, Johan Rosenkilde, and Irene Bouw. Improved power decoding of interleaved one-point Hermitian codes. *Designs, Codes and Cryptography*, 87(2):589–607, 2019.

[23] Hans-Georg Rück and Henning Stichtenoth. A characterization of Hermitian function fields over finite fields. 1994.

[24] Welington Santos. On fractional decoding of Reed-Solomon codes. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 1552–1556. IEEE, 2019.

[25] Georg Schmidt, Vladimir R Sidorenko, and Martin Bossert. Collaborative decoding of interleaved Reed–Solomon codes and concatenated code designs. *IEEE Transactions on Information Theory*, 55(7):2991–3012, 2009.

[26] Henning Stichtenoth. A note on Hermitian codes over GF(q^2). *IEEE Transactions on Information Theory*, 34(5):1345–1348, 1988.

[27] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Heidelberg, Germany, 2^{nd} edition, 2009.

[28] Itzhak Tamo and Alexander Barg. Bounds on locally recoverable codes with multiple recovering sets. In *2014 IEEE International Symposium on Information Theory*, pages 691–695. IEEE, 2014.

[29] Itzhak Tamo and Alexander Barg. A family of optimal locally recoverable codes. *IEEE Transactions on Information Theory*, 60(8):4661–4676, 2014.

[30] Itzhak Tamo, Min Ye, and Alexander Barg. Fractional decoding: Error correction from partial information. In *2017 IEEE International Symposium on Information Theory (ISIT)*, pages 998–1002. IEEE, 2017.

[31] Kyeongcheol Yang and P. Vijay Kumar. On the true minimum distance of Hermitian codes. *Coding Theory and Algebraic Geometry*, pages 99–107, 1992.