Fractional decoding of codes from Hermitian curves

Gretchen L. Matthews
Department of Mathematics
Virginia Tech
Blacksburg, VA 24061 USA
Email: gmatthews@vt.edu

Aidan W. Murphy
Department of Mathematics
Virginia Tech
Blacksburg, VA 24061 USA
Email: awmurphy@vt.edu

Welington Santos
DALTEC/ ASSESSORIA DE MATEMÁTICA
Federal Institute of Santa Catarina
Florianópolis, Santa Catarina 88020-300 Brazil
Email: wsantos.math@gmail.com

***Abstract*—We present a new probabilistic decoding algorithm that can be used to perform fractional decoding of codes from the Hermitian curve. Fractional decoding means that the original codeword may be obtained from a received word using only an α-proportion of symbols of the received word, provided not too many errors have occurred. The procedure presented makes use of fractional decoding of Reed-Solomon codes while allowing for the use of codes of similar lengths over smaller fields.**

I. Introduction

Tamo, Ye, and Barg [1] considered the error correction of maximum distance separable (MDS) codes in the setting in which only part of the received codeword may be downloaded. They also defined the α-decoding radius of an (n, k, l) array code over a finite field $\mathbb{F}_q$. The fractional decoding problem is motivated by the fact that in distributed systems [2] usually there is a limitation on the disk operation as well as on the amount of information transmitted for the purpose of decoding.

In [3], Santos presented a connection between fractional decoding of Reed-Solomon codes and collaborative decoding of interleaved Reed Solomon codes establishing a new fractional decoding procedure. They establish framework and requirements which allow for error correction of a received word using a fraction $\alpha < 1$ of the symbols typically required for decoding of such a code.

In this contribution, we employ the approach in [3] to study the problem of fractional decoding of a family of algebraic geometry codes beyond the Reed-Solomon codes. We study codes from the Hermitian curve and provide a new fractional decoding method for them. While this work focuses on error correction, it is worth noting that some tools are similar to those used in repairing codes, such as those introduced in [4]. In general, Hermitian codes are constructed using smaller alphabets than Reed-Solomon codes of the same lengths; for instance, a Reed-Solomon code of length q^3, where q is a power of a prime, utilizes an alphabet of size q^3 whereas a Hermitian code of the same length is defined using an alphabet of size q^2. Hence, there is an advantage to considering algebraic geometry codes from curves of higher genus.

This work is structured as follows. We close this section with notation. In Section II, the necessary background is provided and preliminary notions are considered. In Section III, we abstract the key ideas from fractional decoding [1] and the fractional decoding problem for Reed Solomon codes [3] which are relevant to our study. Section IV contains our primary contribution where we present a fractional decoding algorithm for Hermitian codes. Section V provides a brief summary and open problems.

Notation: Given $n \in \mathbb{Z}^+$, let $[n] := \{1, 2, \ldots, n\}$ and $\underline{[n]} := \{0, 1, \ldots, n-1\}$. The set of polynomials in indeterminate x with coefficients from a field $\mathbb{F}$ and degree at most $k-1$ is denoted by $\mathbb{F}[x]_{<k}$. The set of $m \times n$ matrices with entries from $\mathbb{F}$ are denoted $\mathbb{F}^{m\times n}$. Given $A \in \mathbb{F}^{m\times n}$, $Row_i(A)$ denotes the i^{th} row of A; in this paper, rows are typically indexed by $\underline{[m]}$ and columns by $[n]$.

II. Preliminaries

Let $\mathbb{F}_q$ denote the finite field with q elements, and consider its degree l extension $\mathbb{F}_{q^l}$:

$$\begin{array}{c} \mathbb{F}_{q^l} \\ l \,| \\ \mathbb{F}_q. \end{array}$$

For each $a \in \mathbb{F}_{q^l}$, the trace of a with respect to the extension $\mathbb{F}_{q^l}/\mathbb{F}_q$ is

$$tr(a) = a + a^q + a^{q^2} + \cdots + a^{q^{l-1}} \in \mathbb{F}_q.$$

The work of the first author is supported in part by NSF under Grant DMS-1855136 and in part by the Commonwealth Cyber Initiative.

Fix a basis $\mathcal{B} := \{\zeta_0, \ldots, \zeta_{l-1}\}$ of $\mathbb{F}_{q^l}/\mathbb{F}_q$. Then each $a \in \mathbb{F}_{q^l}$ can be expressed as a linear combination of the l elements of $\mathcal{B}$ using coefficients from $\mathbb{F}_q$; that is, each element of $\mathbb{F}_{q^l}$ can be expressed using l elements of $\mathbb{F}_q$. As noted in [5, Definition 2.30] for each $a \in \mathbb{F}_{q^l}$,

$$a = \sum_{i=0}^{l-1} tr\left(\zeta_i a\right) \nu_i$$

where $\{\nu_0, \ldots, \nu_{l-1}\}$ is the dual basis of $\mathcal{B}$.

Given $h(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} \in \mathbb{F}_{q^l}[x]_{<k}$ and $i \in \underline{[l]}$, let

$$h_i(x) = \sum_{u=0}^{k-1} tr\left(\zeta_i a_u\right) x^u \in \mathbb{F}_q[x]_{<k}. \tag{1}$$

It is immediate that $h(x)$ can be recovered from $\{h_i(x) : i \in [l]\}$ since

$$\begin{array}{rcl} \sum_{i=0}^{l-1} \nu_i h_i(x) & = & \sum_{i=0}^{l-1} \nu_i \left(\sum_{u=0}^{k-1} tr\left(\zeta_i a_u\right) x^u \right) \\ & = & \sum_{u=0}^{k-1} \left(\sum_{i=0}^{l-1} tr\left(\zeta_i a_u\right) \nu_i \right) x^u \\ & = & \sum_{u=0}^{k-1} a_u x^u = h(x). \end{array}$$

In this paper, we will employ Reed-Solomon codes in our approach to decoding codes from the Hermitian curve. Given $\Gamma := \{\gamma_1, \ldots, \gamma_n\} \subseteq \mathbb{F}_{q^l}$ and $k \in \mathbb{Z}^+$ so that $k < n$, $RS(q^l, n, k) =$

$$\left\{ \left(f(\gamma_1), f(\gamma_2), \ldots, f(\gamma_n)\right) : f \in \mathbb{F}_{q^l}[x]_{<k} \right\} \subseteq \mathbb{F}_{q^l}^n$$

is a Reed-Solomon code. The code $RS(q^l, n, k)$ is the image of the evaluation map $ev : \mathbb{F}_{q^l}[x]_{<k} \to \mathbb{F}_{q^l}^n$ given by $ev(f) := (f(\gamma_1), f(\gamma_2), \ldots, f(\gamma_n))$. To emphasize the evaluation set, codewords are sometimes expressed as $f(\Gamma) := ev(f)$.

The focus of this work is decoding certain Hermitian codes, which we define presently; see [6] for additional details. Consider the Hermitian curve $\mathcal{H}_q$ given by $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^{2l}}$. The field of rational functions on $\mathcal{H}_q$ over $\mathbb{F}_{q^{2l}}$ is denoted $\mathbb{F}_{q^{2l}}(\mathcal{H}_q)$. At times, we may wish to consider the field of rational functions of $\mathcal{H}_q$ over a subfield K of $\mathbb{F}_{q^{2l}}$, denoted $K(\mathcal{H}_q)$. We will consider the base field for $\mathcal{H}_q$ to be $\mathbb{F}_{q^2}$ as the curve is maximal over this field. Hence, we will make use of the extension

$$\begin{array}{l} \mathbb{F}_{q^{2l}} \\ l \,| \\ \mathbb{F}_{q^2} \end{array}$$

when considering Hermitian codes. Given $a \in \mathbb{F}_{q^2}$, let

$$\Gamma_a := \left\{ b \in \mathbb{F}_{q^2} : b^q + b = a^{q+1} \right\}.$$

It is well known that for all $a \in \mathbb{F}_{q^2}$, $\mid \Gamma_a \mid = q$, and the affine points of $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$ are of the form $P_{ab} := (a, b)$ with $a \in \mathbb{F}_{q^2}$ and $b \in \Gamma_a$; that is, the set of $\mathbb{F}_{q^2}$-rational points of $\mathcal{H}_q$ is $\mathcal{H}_q(\mathbb{F}_{q^2}) := \left\{ P_{ab} : a \in \mathbb{F}_{q^2}, b \in \Gamma_a \right\} \cup \{P_\infty\}$ where P_∞ denotes the unique point at infinity. It is useful to partition $\mathcal{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ as

$$\mathcal{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\} = \dot{\cup}_{a \in \mathbb{F}_{q^2}} P_a$$

where $P_a := \{P_{ab} : b \in \Gamma_a\}$.

In this paper, we consider Hermitian codes

$$C(\beta P_\infty) = \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(\beta P_\infty)\}$$

where $\{P_1, \ldots, P_n\} = \mathcal{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ and

$$\mathcal{L}(\beta P_\infty) = \left\langle \begin{array}{ll} x^i y^j : & 0 \le i, 0 \le j \le q-1, \\ & iq + j(q+1) \le \beta \end{array} \right\rangle. \tag{2}$$

It is immediate that $C(\beta P_\infty)$ is the image of the evaluation map $ev : \mathcal{L}(\beta P_\infty) \to \mathbb{F}_{q^{2l}}^n$ defined by $ev(f) = (f(P_1), \ldots, f(P_n))$. The points $P_1, \ldots, P_n$ are called evaluation points of the code. If $q(q-1) \le \beta < q^3$, then $C(D, \beta P_\infty)$ is a $[q^3, \beta + 1 - \frac{q(q-1)}{2}, \geq q^3 - \beta]$ code; the exact minimum distance may be found in [7].

Some notions introduced below apply to more general families of algebraic geometry codes. We note that in all that follows, it is important that codewords arise via evaluation of rational functions which are in fact polynomials in $\mathbb{F}_{q^{2l}}[x, y]$.

III. Fractional decoding of Reed-Solomon codes

In this section, we consider the α-decoding problem in which a decoder downloads an α proportion of each of the codeword's coordinates. Given an (n, k)-linear code, notice that we must have $\alpha \geqslant \frac{k}{n}$. Because the codeword encodes k data symbols, as many symbols are needed to recover the data even without errors. Setting $\alpha = 1$ yields the standard decoding problem. Hence, the goal of fractional decoding is study error correction for α in the range $\frac{k}{n} \leqslant \alpha < 1$.

It was shown in [1] that the maximum errors that an (n, k)-linear code C can correct by downloading a α-proportion of each of its codeword's coordinates is upper bounded by the α-decoding radius of C

$$\tau_\alpha = \left\lfloor \frac{n - k/\alpha}{2} \right\rfloor; \tag{3}$$

moreover, an $RS(q^l, n, k, \mathcal{L})$ code with $\mathcal{L} \subseteq \mathbb{F}_q$ achieves the optimal α-decoding radius (3).

Our procedure for fractional decoding of codes from Hermitian curves makes use of that for Reed-Solomon

codes, as introduced in [3]. Below, we abstract and further develop the necessary ideas for this application.

Suppose $\Gamma := \{\gamma_1, \ldots, \gamma_n\} \subseteq \mathbb{F}_q$, $\alpha = \frac{m}{l}$ where $m \in \mathbb{Z}^+$ such that $m < l$ and $m \mid k$,

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

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

$$p_j(x) := \prod_{a \in A_j} x - a \in \mathbb{F}_q[x]. \tag{4}$$

Then $p_j(a) = 0$ for all $a \in A_j$ and $\deg p_j(x) = |A_j|$. For $h(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} \in \mathbb{F}_{q^l}[x]_{<k}$ and for $j \in \underline{[m]}$, set

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

where $k_j := \mid A_j \mid (l-m)(j+1) + k$. Hence, $ev\left(T_j(h)(x)\right) \in RS(q, n, k_j)$ Consequently, for each $j \in \underline{[m]}$,

$$\begin{aligned} &h(\Gamma) \in RS(q^l, n, k) \subseteq \mathbb{F}_{q^l}^n \\ &\Rightarrow T_j(h)(\Gamma) \in RS(q, n, k_j) \subseteq \mathbb{F}_q^n. \end{aligned}$$

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

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

In this setting, one may consider the virtual projection of $C = RS(q^l, n, k)$ is the interleaved Reed-Solomon code

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

as defined in [3]. With this in mind, we make the following definition.

Definition 1. The virtual projection of $y \in \mathbb{F}_{q^l}^n$ is

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

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

$$\begin{aligned} d_i^j : \quad = \quad & tr\left(\zeta_{l-m+j} y_i\right) \left(p_j(\gamma_i)\right)^{(l-m)(j+1)} \\ & + \sum_{u=0}^{l-m-1} tr\left(\zeta_u y_i\right) \left(p_j(\gamma_i)\right)^{u(j+1)} \in \mathbb{F}_q. \end{aligned}$$

Notice that the virtual projection of a codeword $c := ev(h) \in RS(q^l, n, k)$ is

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

which may be viewed as a codeword of an interleaved Reed-Solomon code.

We now review the fractional decoding procedure for Reed-Solomon codes introduced in [3] employing collaborative decoding as in [8].

Suppose $y \in \mathbb{F}_{q^l}^n$ is received and $y = c + e$ where $c \in RS(q^l, n, k)$, and $wt(e) \leq t$,

$$t \leq \frac{m}{m+1} \left(n - k - \frac{l-m}{m} \sum_{j=0}^{m-1} \mid A_j \mid (j+1) \right).$$

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

$$S_{js} := d_{k_j + s}^j.$$

Notice that the values $S_{j0}, S_{j1}, \ldots, S_{jn-k_j-1}$ are precisely the last $n - k_j$ entries of row j of the matrix $\pi(y)$ (where the rows are enumerated using elements of $\underline{[m]}$). Consequently, the desired syndromes may be read off directly from a block upper-triangular submatrix of $\pi(y)$: the last $n - k_0$ entries of $Row_0\pi(y)$, the last $n - k_1$ entries of $Row_1\pi(y)$, and so on until the last $n - k_{m-1}$ entries of $Row_{m-1}\pi(y)$. Associate with each $j \in \underline{[m]}$, $S^{(j)} :=$

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

and

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

Setting

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

and

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

allows for the formation of the linear system

$$S\Lambda = U$$

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

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

As described in [8], this gives rise to the error locator polynomial $E(x) = 1 + \sum_{i=1}^{t} \Lambda_i x^i$ which if separable over $\mathbb{F}_q$ allows for correction of the up to t incorrect values and otherwise leads to a decoding failure.

The procedure for fractional decoding of a Reed-Solomon code can be summarized as follows. Given a received word $y \in \mathbb{F}_{q^l}^n$:

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

Errors in the interleaved Reed-Solomon code obtained in this procedure are independent random vectors uniformly distributed over $F_q^m \backslash \{0\}$. This is due to the fact that each symbol in an erroneous column i of C_P is given by $T_j(e)(\Gamma_i)$, $j \in \underline{[m]}$, and each T_j do not depend on each other. So, [3, Theorem 13], proven that this procedure corrects $t \leq \tau_\alpha$ errors with failure probability $P_{f\alpha}$ where $\tau_\alpha := \frac{1}{m+1}\left(mn + k\binom{m}{2} - \frac{k}{\alpha}\binom{m+1}{2}\right)$ and

$$P_{f\alpha} \leq \left(\frac{q^m - \frac{1}{q}}{q^m - 1}\right)^t \frac{q^{-(m+1)(\tau_\alpha - t)}}{q-1}$$

provided $\frac{k}{n} \leq \frac{m}{m(l-m)+l}$. Notice that $\alpha l n$ symbols of $\mathbb{F}_q$ are used in this error correction procedure which is strictly less than ln symbols typically used.

IV. Hermitian codes and fractional decoding

In this section, we consider fractional decoding of certain Hermitian codes.

First, consider the situation in which $f \in \mathcal{L}(\beta P_\infty) \subseteq \mathbb{F}_{q^{2l}}(\mathcal{H}_q)$. Suppose there exist $a_{ij} \in \mathbb{F}_{q^{2l}}$ such that

$$f(x,y) = \sum_{j=0}^{r-1} \sum_{i=0}^{\lfloor \frac{\beta - j(q+1)}{q} \rfloor} a_{ij} x^i y^j \in \mathbb{F}_{q^{2l}}[x,y] \tag{5}$$

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

$${}_af := f(a,y) \in \mathbb{F}_{q^{2l}}[y]_{<r}.$$

It is convenient to enumerate the elements of $\mathbb{F}_{q^2}$: $a_1, \ldots, a_{q^2}$ and fix this ordering in the discussion that follows. In particular, we assume that the evaluation points of $C(\beta P_\infty)$ are ordered so that

$$(P_1, \ldots, P_n) = \left((P_{a_i b})_{b\in\Gamma_{a_i}}\right)_{i=1}^{q^2} \tag{6}$$

which allows the codeword $ev(f)$ to be viewed (by slight abuse of notation) as

$$ev(f) = \left({}_{a_1}f(\Gamma_{a_1}) \quad {}_{a_2}f(\Gamma_{a_2}) \quad \cdots \quad {}_{a_{q^2}}f(\Gamma_{a_{q^2}})\right).$$

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

$${}_{a_i}f(\Gamma_{a_i}) \in RS(q^{2l}, q, r).$$

Inspired by Section III, for each $i \in [q^2]$, define subsets $A_{ij} \subseteq \mathbb{F}_{q^2}$ so that

$$\Gamma_{a_i} \subseteq \bigdot\bigcup_{j=0}^{m-1} A_{ij} \subseteq \mathbb{F}_{q^2}. \tag{7}$$

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

$$p_{ij}(y) := \prod_{b\in A_{ij}} (y-b)$$

and $T_{i,j}(f)(y) \in \mathbb{F}_{q^2}[y]_{<k_{ij}}$ by

$$\begin{aligned} T_{i,j}(f)(y) = {}& {}_{a_i}f_{l-m+j}(y)\left(p_{ij}(y)\right)^{(l-m)(j+1)} \\ & + \sum_{u=0}^{l-m-1} {}_{a_i}f_u(y)\left(p_{ij}(y)\right)^{u(j+1)} \end{aligned} \tag{8}$$

where for $u \in \underline{[m]}$, ${}_{a_i}f_u$ is defined as in (1) and

$$k_{ij} := \mid A_{ij} \mid (l-m)(j+1) + r,$$

for all $i \in [q^2]$ and $j \in \underline{[m]}$. Then $T_{i,j}(f)(\Gamma_{a_i})$ is a codeword of an Reed-Solomon code $RS(q^2, q, k_{ij})$.

Definition 2. Suppose $f \in \mathcal{L}(\beta P_\infty)$ as in (5). The virtual projection of f is the matrix $\rho(f) \in \mathbb{F}_{q^2}^{m\times n}$ given by

$$\rho(f) := \begin{bmatrix} T_{1,0}(f)(\Gamma_{a_1}) & \cdots & T_{q^2,0}(f)(\Gamma_{a_{q^2}}) \\ T_{1,1}(f)(\Gamma_{a_1}) & \cdots & T_{q^2,1}(f)(\Gamma_{a_{q^2}}) \\ \vdots & & \vdots \\ T_{1,m-1}(f)(\Gamma_{a_1}) & \cdots & T_{q^2,m-1}(f)(\Gamma_{a_{q^2}}) \end{bmatrix}.$$

Note that the virtual projection of f is expressed using $mn = \alpha ln$ elements of $\mathbb{F}_{q^2}$ whereas $ev(f)$ itself is described using ln elements of $\mathbb{F}_{q^2}$. Even so, we will see that f (and hence $ev(f)$) can be recovered from $\rho(f)$ with high probability.

Next, note that for each $i \in [q^2]$, ${}_{a_i}f$ can be recovered from $\rho(f)$; in fact, recovery of ${}_{a_i}f$ only depends on knowledge of

$$\rho(f) \mid_{\Gamma_{a_i}} = \begin{bmatrix} T_{i,0}(f)(\Gamma_{a_i}) \\ T_{i,1}(f)(\Gamma_{a_i}) \\ \vdots \\ T_{i,m-1}(f)(\Gamma_{a_i}) \end{bmatrix} \in \mathbb{F}_{q^2}^{m \times q}, \quad (9)$$

an $m \times q$ submatrix of $\rho(f)$. Indeed, $\rho(f) \mid_{\Gamma_{a_i}}$ is the virtual projection of the codeword

$$ev({}_{a_i}f) =_{a_i} f(\Gamma_{a_i}) \in RS(q^{2l}, q, r).$$

Then [3, Lemma 10] applies to determine ${}_{a_i}f$ for all $i \in [q^2]$. It remains to determine f.

Notice that the number of terms of f is at most

$$\begin{aligned} \sum_{j=0}^{r-1} \sum_{i=0}^{\lfloor \frac{\beta - j(q+1)}{q} \rfloor} 1 &\leq \alpha + q - \tfrac{q+1}{q} \sum_{i=0}^{q-1} i \\ &= \alpha + q - \tfrac{q^2}{2} < \alpha < q^3. \end{aligned}$$

From ${}_{a_i}f(y)$, $i \in [q^2]$, q^3 interpolation points can be determined since ${}_{a_i}f(y) = f(a_i, y)$ and

$$f(a_i, b) =_{a_i} f(b) \in \mathbb{F}_{q^{2l}}$$

for all $b \in \Gamma_{a_i}$. As a result, f can be recovered with high probability from ${}_{a_i}f(y)$, $i \in [q^2]$.

Next, we define the virtual projection of a vector $y \in \mathbb{F}_{q^{2l}}^n$. For $i \in [q^2]$, write

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

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

$$\begin{aligned} d_{is}^j = &tr\left(\zeta_{l-m+j} y_i\right) \left(p_{ij}(b_{is})\right)^{(l-m)(j+1)} \\ &+ \sum_{u=0}^{l-m-1} tr\left(\zeta_u y_i\right) \left(p_{ij}(b_{is})\right)^{u(j+1)} \in \mathbb{F}_{q^2}. \quad (10) \end{aligned}$$

Definition 3. The virtual projection of $y \in \mathbb{F}_{q^{2l}}^n$ is

$$\pi(y) := \left[D_1 \mid D_2 \mid \cdots \mid D_{q^2}\right] \in \mathbb{F}_{q^2}^{m \times n}$$

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 $i \in [q^2]$.

Note that the virtual projection of y consists of mn entries of $\mathbb{F}_{q^2}$, whereas y is typically described using mnl entries of this field. It can be verified that the virtual projection of a codeword $c := ev(f) \in C(\beta P_\infty)$ satisfies

$$\rho(f) = \pi(ev(f)).$$

Moreover, for each $i \in [q^2]$, $D_i = \rho(f) \mid_{\Gamma_{a_i}}$ as given in (9).

Finally, we are ready to describe the decoding procedure.

Algorithm 1: Virtual Projection of Hermitian codes IRS Decoder

Input: Received word $y = ev(f) + e$ where $f \in \mathcal{L}(\beta P_\infty)$ as in (5) and $\alpha = m/l$.
For: $i \in [q^2]$, and $j \in \underline{[m]}$ **do**
Download the entries of the virtual projetion $\pi(y) \in \mathbb{F}_{q^2}^{m \times n}$.
For each submatrix D_i of $\pi(y)$ apply the algorithm summarized in Section III to recover ${}_{a_i}f$.
if ${}_{a_i}f$ *is successfully recovered for all* $i \in [q^2]$ **then**
  for each $s \in [q]$ **do**
  Calculate the points

$$(a_i, {}_{a_i} f(b_{is})).$$

  Use the pairs of the field elements obtained in the previous step to determine $f \in \mathcal{L}(\beta P_\infty)$.
else
  decoding failure
output: $f \in \mathcal{L}(\beta P_\infty)$ or decoding failure

Notice that the above decoding algorithm operates using αln elements of $\mathbb{F}_{q^2}$ rather than the ln symbols of $\mathbb{F}_{q^2}$ typically used in error correction for this Hermitian codes. With this algorithm we can correct t errors, where

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

where τ_{α_i} is the decoding radius associated with the submatrix D_i and the exact value of t will depend on the error locations.

V. Conclusion

In this paper, we considered fractional decoding of codes from Hermitian curves. This is a first step in fractional decoding of algebraic geometry codes beyond Reed-Solomon codes. It would be interesting to explore the α-decoding radius for these codes. It also remains to determine the full error correcting capability of the fractional decoding procedure considered here.

REFERENCES

[1] I. Tamo, M. Ye, and A. Barg, Fractional Decoding: Error Correction from Partial Information, in Proc. 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, pp. 998-1002, 2017. doi:https://doi.org/10.1109/ISIT.2017.8006678.

[2] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, Network Coding for Distributed Storage Systems, IEEE Trans. Inform. Theory, vol. 56, no. 9, pp. 4539-4551, 2010. doi: https://doi.org/10.1109/TIT.2010.2054295

[3] W. Santos, On Fractional Decoding of Reed-Solomon Codes, 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, pp. 1552-1556, 2019. doi: 10.1109/ISIT.2019.8849787.

[4] V. Guruswami and M. Wootters, Repairing Reed-Solomon Codes, in IEEE Trans. Inform. Theory, vol. 63, no. 9, pp. 5684-5698, 2017, doi: 10.1109/TIT.2017.2702660.

[5] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications. Cambridge: Cambridge University Press. 1994. doi:10.1017/cbo9781139172769.

[6] H. Stichtenoth, A note on Hermitian codes over $GF(q^2)$, in IEEE Trans. Inform. Theory, vol. 34, no. 5, pp. 1345-1348, 1988, doi: 10.1109/18.21267.

[7] K. Yang and P. V. Kumar, On the true minimum distance of Hermitian codes. In: Stichtenoth H., Tsfasman M.A. (eds) Coding Theory and Algebraic Geometry. Lecture Notes in Mathematics, vol 1518. Springer, Berlin, Heidelberg, 1992. https://doi.org/10.1007/BFb0087995

[8] G. Schmidt, V. R. Sidorenko and M. Bossert, Collaborative Decoding of Interleaved Reed–Solomon Codes and Concatenated Code Designs, in IEEE Trans. Inform. Theory, vol. 55, no. 7, pp. 2991-3012, 2009, doi: 10.1109/TIT.2009.2021308.

[9] A. Brown, L. Minder, and Amin Shokrallahi. Improved decoding of interleaved AG codes, IMA International Conference on Cryptography and Coding. Springer, Berlin, Heidelbert, 2005.

[10] S. Kampf. Bounds on collaborating decoding of interleaved Hermitian codes and virtual extension, Designs, Codes and Cryptography vol. 70, no. 1, pp. 9-25, 2014.

[11] S. Puchinger, J. Rosenkilde, and I. Bouw. Improved power decoding of interleaved one-point Hermitian codes, Designs, Codes and Cryptography vol. 55, no. 2, pp. 588-607, 2019.

[12] J. Ren, On the Structure of Hermitian Codes and Decoding for Burst Errors, IEEE Trans. Inform. Theory, vol. 50, no. 11, pp. 2850-2854, 2004. doi: https://doi.org/10.1109/TIT.2004.836918