Fractional decoding of r-Hermitian codes

Gretchen L. Matthews*[1], Aidan W. Murphy†[2], and Welington Santos‡[3]

[1,3]Department of Mathematics, Virginia Tech
[2]Johns Hopkins Applied Physics Laboratory

Abstract

In this paper, we present a fractional decoding algorithm for a new family of codes which are constructed from the Hermitian curve, called r-Hermitian codes. These codes of length n are defined over an extension field $\mathbb{F}_{q^{2\ell}}$ of $\mathbb{F}_{q^2}$ and the fractional decoding algorithms that we present are algorithms for error correction that use only $\alpha\ell n$ symbols of a subfield of size q^2 as input into the decoding algorithm, where $\alpha < 1$, meaning a fraction of the subsymbols that are typically utilized. We demonstrate that collaborative decoding of interleaved codes supports fractional decoding of the r-Hermitian codes, allowing for improved bounds on the fractional decoding radius.

keywords: *distributed storage system, fractional decoding, Hermitian curve, collaborative decoding, interleaved code, Reed-Solomon code*

1 Introduction

Distributed storage systems [1] are the infrastructure for cloud computing service providers. In a distributed storage system, a data file is encoded and distributed to n nodes in such a way that a data collector can decode the original file by downloading from k nodes. The common coding schemes employed in distributed storage systems include replication schemes in Google File Systems [3], erasure codes in Oceanstore [6] and locally reparable codes in Windows Azure [5].

Recently, Tamo, Ye, and Barg [12] considered error correction by maximum distance separable (MDS) codes based on part of the received codeword, defining the fractional decoding problem and the α-decoding radius of an array code over a finite field $\mathbb{F}_q$. The fractional decoding problem is motivated by the fact that in distributed systems there is usually a limitation on the disk operation as well as on the amount of information transmitted for the purpose of decoding. Sometimes thought of as error correction with partial information, fractional decoding considers codes defined over an extension field and algorithms for error correction that use fewer symbols from the base field than is typical, thus operating using a restricted amount of information in the decoding process.

In this paper, we present a fractional decoding algorithm for a new family of codes, called r-Hermitian codes, which are constructed from a particular higher genus curve, the Hermitian curve. To our knowledge, it is the first fractional decoding algorithm for codes from curves of positive genus. In [9] Santos provided a connection between fractional decoding of Reed-Solomon codes, which can be considered as codes from a curve of genus 0, the projective line, and collaborative decoding of interleaved Reed-Solomon codes. The codes considered in this paper are defined using the Hermitian curve $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$, an integer $r < q$, and a constant field extension of the Riemann-Roch space of a divisor on this curve. They may be considered as evaluation codes with

*gmatthews@vt.edu
†Aidan.Murphy@jhuapl.edu
‡welington@vt.edu

The work of the first and third author is supported in part by NSF DMS-1855136. The first author is also supported in part by the Commonwealth Cyber Initiative and NSF DMS-2201075. This work was performed while the second author was at Virginia Tech. Some results from Section 3.2 of this paper were presented at ISIT 2021.

evaluation points whose coordinates lie in the subfield $\mathbb{F}_{q^2}$. Taking evaluation points in a base field to define a family of codes for particular purpose is an idea utilized by Guruswami and Xing [4] and Gao, Yue, Huang, and Zhang [2] among others (including [7]). The r-Hermitian codes are described in Section 2.

Both r-Hermitian codes and those considered in [12] have length q^3, over alphabet sizes q^{2l} and q^{3l} respectively. While both are shorter than Reed-Solomon codes over the same alphabets for $l > 1$, both allow for fractional decoding with $\alpha < 1$ whereas Reed-Solomon codes themselves do not. Several approaches are utilized to provide probabilistic algorithms for fractional decoding of r-Hermitian codes. The first, given in Section 3, is rather naive but sets the notation to be used for more sophisticated approaches later in the paper. The remaining algorithms, featured in Section 4 are based on collaborative decoding of interleaved codes. It is important to note that these results are different from collaborative decoding of interleaved Hermitian codes. The codes considered in this paper are subcodes of a constant field extension of the traditional one-point Hermitian code to $\mathbb{F}_{q^{2l}}$ but are not interleaved Hermitian codes. Algorithm 3 employs homogeneous interleaved Reed-Solomon codes and can correct $\frac{m}{m+1}\left(q - \frac{r}{\alpha}\right)$ errors by downloading an α-proportion of the received word. This upper bound is improved to $\frac{q^2 m}{m+1}\left(q - \frac{r}{\alpha}\right)$ if the errors are well distributed. In comparison, Algorithm 4 utilizes heterogeneous interleaved Reed-Solomon codes and can correct $\frac{1}{m+1}\left[mq - \frac{r}{\alpha}\binom{m+1}{2} + r\binom{m}{2}\right]$ errors. This bound is improved to $\frac{q^2}{m+1}\left[mq - \frac{r}{\alpha}\binom{m+1}{2} + r\binom{m}{2}\right]$ if the errors are well distributed. We prove that the approach via heterogeneous interleaved Reed-Solomon codes (Algorithm 4) corrects more errors than via homogeneous interleaved Reed-Solomon codes (Algorithm 3) if and only if $m \geq \frac{1+\sqrt{1+4l}}{2}$. The paper ends with a conclusion in Section 5.

2 Codes with evaluation points in a subfield and r-Hermitian codes

Guruswami and Xing [4] considered Reed-Solomon codes whose evaluation points belong to a subfield and provided a list decoding algorithm for those codes that can correct a fraction of errors approaching the code minimum distance. Those codes are defined as follows.

Let l a positive integer and n, k be positive integers satisfying $1 \leq k < n \leq q$. The Reed-Solomon code $\mathcal{RS}^{(q,l)}[n,k]$ is a code over the alphabet $\mathbb{F}_{q^l}$ that encodes a polynomial $f \in \mathbb{F}_{q^l}[x]$ of degree at most $k-1$ as

$$f(x) \mapsto (f(\omega_1), f(\omega_2), \ldots, f(\omega_n)), \tag{2.1}$$

where $\mathcal{L} = \{\omega_1, \ldots, \omega_n\} \subseteq \mathbb{F}_q$. Note that if $\mathcal{C} \subseteq \mathbb{F}_{q^l}^n$ is an $[n,k]$ linear code, then $\mathcal{C}$ can be seen as an (n,k,l) array code $\mathcal{C}' \subseteq \mathbb{F}_q^{l \times n}$. An (n,k,l) array code $\mathcal{C}$ over a finite field $\mathbb{F}_q$ maps an $l \times k$ data matrix $D = (D_1, \ldots, D_k) \in \left(\mathbb{F}_q^l\right)^k$ to an $l \times n$ codeword matrix $C = (C_1, \ldots, C_n) \in \left(\mathbb{F}_q^l\right)^n$. The array code $\mathcal{C}$ may be seen as the image of a map

$$\begin{array}{rccc} \phi: & \mathbb{F}_q^{l\times k} & \to & \mathbb{F}_q^{l\times n} \\ & D & \mapsto & C \end{array}.$$

Each column vector C_i of the matrix corresponds to a codeword coordinate so that the coordinates are indexed by $[n] := \{1, \ldots, n\}$. The parameter l is called the *sub-packetization* of $\mathcal{C}$, and the code is said to have length n. Indeed, given a basis $\{\zeta_0, \ldots, \zeta_{l-1}\}$ of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$, let $\{\nu_0, \nu_1, \ldots, \nu_{l-1}\}$ be its trace-dual basis. Then every element $\beta \in \mathbb{F}_{q^l}$ can be written as

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

where tr denotes the trace relative to the extension $\mathbb{F}_{q^l}/\mathbb{F}_q$. The codeword $c = (c_1, \ldots, c_n) \in \mathcal{C} \subseteq \mathbb{F}_{q^l}^n$ can be viewed as

$$C = \begin{bmatrix} tr(\zeta_0 c_1) & tr(\zeta_0 c_2) & \cdots & tr(\zeta_0 c_n) \\ tr(\zeta_1 c_1) & tr(\zeta_1 c_2) & \cdots & tr(\zeta_1 c_n) \\ \vdots & \vdots & \ddots & \vdots \\ tr(\zeta_{l-1} c_1) & tr(\zeta_{l-1} c_2) & \cdots & tr(\zeta_{l-1} c_n) \end{bmatrix} \in \mathcal{C}' \subseteq \mathbb{F}_q^{l \times n}.$$

Taking this into account, Tamo, Ye, and Barg [12] show that $\mathcal{RS}^{(q,l)}[n,k]$ codes are optimal for fractional decoding in the sense that $\left\lfloor \frac{n-\frac{k}{\alpha}}{2} \right\rfloor$ errors may be corrected by downloading αln of $\mathbb{F}_q$. Because a received word has n coordinates in $\mathbb{F}_{q^l}$, which can be expressed using nl symbols of $\mathbb{F}_q$ and αln symbols that depend on these received symbols are downloaded, we say here (and in similar situations throughout) that an α-proportion of symbols are used in decoding.

Also in [4], V. Guruswami and Xing considered algebraic-geometric codes whose evaluation points belong to a subfield and provided a list decoding algorithm to those codes. Here, we focus our attention on codes from the Hermitian curve, which has produced the best understood family of algebraic geometry codes beyond Reed-Solomon codes.

Let $\mathcal{H}_q$ be the Hermitian curve given by $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$. Let $P_\infty, P_1, \ldots, P_n$ be its $n+1$ distinct $\mathbb{F}_{q^2}$-rational places so that $n = q^3$. Given $a \in \mathbb{F}_{q^2}$, consider $\Gamma_a := \left\{ b \in \mathbb{F}_{q^2} \,:\, b^q + b = a^{q+1} \right\}$. It is well known that for all $a \in \mathbb{F}_{q^2}$, $|\Gamma_a| = q$ and that 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 places of $\mathcal{H}_q$ is

$$\mathcal{H}_q(\mathbb{F}_{q^2}) := \left\{ P_{ab} : a \in \mathbb{F}_{q^2}, b \in \Gamma_a \right\} \cup \left\{ P_\infty \right\},$$

where P_∞ denotes the unique point at infinity which has projective coordinates $(0:1:0)$. It is useful to partition $\mathcal{H}_q(\mathbb{F}_{q^2}) \setminus \{P_\infty\}$ as

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

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

Next, we consider functions that will be useful in the code constructions. Recall that the Riemann-Roch space of a divisor βP_∞ on $\mathcal{H}_q$ is

$$\mathcal{L}(\beta P_\infty) = \left\langle x^i y^j : 0 \le i, 0 \le j \le q-1, iq + j(q+1) \le \beta \right\rangle \subseteq \mathbb{F}_{q^2}[x,y].$$

Let $\mathcal{L}_l(\beta P_\infty)$ be the Riemann-Roch space of the divisor βP_∞ on $\mathcal{H}_q$ over $\mathbb{F}_{q^{2l}}$. It is well-known that

$$\mathcal{L}_l(\beta P_\infty) = \mathcal{L}(\beta P_\infty) \otimes \mathbb{F}_{q^{2l}}.$$

This implies that $\dim_{\mathbb{F}_{q^{2l}}} \mathcal{L}_l(\beta P_\infty) = \dim_{\mathbb{F}_{q^2}} \mathcal{L}(\beta P_\infty)$ and a basis of $\mathcal{L}(\beta P_\infty)$ over $\mathbb{F}_{q^2}$ is a basis of $\mathcal{L}_l(\beta P_\infty)$ over $\mathbb{F}_{q^{2l}}$; that is,

$$\mathcal{L}_l(\beta P_\infty) = \left\langle x^i y^j : 0 \le i, 0 \le j \le q-1, iq + j(q+1) \le \beta \right\rangle \subseteq \mathbb{F}_{q^{2l}}[x,y].$$

Define the constant extension to $\mathbb{F}_{q^{2l}}$ of the Hermitian code $\mathcal{C}(\beta P_\infty) \subset \mathbb{F}_{q^2}^n$ to be

$$\mathcal{C}_l(\beta P_\infty) = \{(f(P_1), f(P_2), \ldots, f(P_n)) : f \in \mathcal{L}_l(\beta P_\infty)\} \subseteq \mathbb{F}_{q^{2l}}^n.$$

According to [4, Lemma 4.6], if $q(q-1) \le \beta < q^3$, $\mathcal{C}_l(\beta P_\infty)$ is an $\mathbb{F}_{q^{2l}}$-linear code over $\mathbb{F}_{q^{2l}}$, with dimension at least $\beta + 1 - \frac{q(q+1)}{2}$ and minimum distance at least $n - \beta$.

For a fixed $r \in \mathbb{Z}$, $1 \le r \le q$ we define

$$\mathcal{L}_l(\beta P_\infty, r) := \left\{ \sum_{j=0}^{r-1} \sum_{i=0}^{s_j} a_{ij} x^i y^j : a_{ij} \in \mathbb{F}_{q^{2l}} \right\} \subseteq \mathcal{L}_l(\beta P_\infty),$$

where $s_j = \left\lfloor \frac{\beta - j(q+1)}{q} \right\rfloor$.
Note that if $r = 1$, then

$$\mathcal{L}_l(\beta P_\infty, 1) = \left\{ \sum_{i=0}^{\lfloor \frac{\beta}{q} \rfloor} a_{ij} x^i : a_{ij} \in \mathbb{F}_{q^{2l}} \right\} \subseteq \mathbb{F}_{q^{2l}}[x]$$

and if $r = q$,

$$\mathcal{L}_l(\beta P_\infty, q) = \mathcal{L}_l(\beta P_\infty).$$

Moreover, there is a nesting

$$\mathcal{L}_l(\beta P_\infty, 1) \subseteq \mathcal{L}_l(\beta P_\infty, 2) \subseteq \cdots \subseteq \mathcal{L}_l(\beta P_\infty, q-1) \subseteq \mathcal{L}_l(\beta P_\infty, q) = \mathcal{L}_l(\beta P_\infty).$$

Now, we are set to define the r-Hermitian codes.

Definition 1. *Let $r, l \in \mathbb{Z}$, $1 \leq r \leq q$. An r-Hermitian code over $\mathbb{F}_{q^{2l}}$ is defined as*

$$\mathcal{C}(\beta P_\infty, r) = \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}_l(\beta P_\infty, r)\} \subseteq \mathbb{F}_{q^{2l}}^n.$$

It is immediate that $\mathcal{C}(\beta P_\infty, r)$ is the image of the evaluation map

$$\begin{array}{rccc} ev: & \mathcal{L}_l(\beta P_\infty, r) & \to & \mathbb{F}_{q^{2l}}^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)). \end{array}$$

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

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

Note that given $(c_1, \ldots, c_n) \in \mathcal{C}(\beta P_\infty, r)$, there exists

$$f(x, y) = \sum_{j=0}^{r-1} \sum_{i=0}^{s_j} a_{ij} x^i y^j \in \mathcal{L}(\beta P_\infty, r) \tag{2.2}$$

such that $c_i = f(P_i)$ for all $i \in [n]$. Moreover, by a slight abuse of notation, $(f(P_1), \ldots, f(P_n))$ can be viewed as

$$\left({}_{a_1} f(\Gamma_{a_1}), {}_{a_2} f(\Gamma_{a_2}), \ldots, {}_{a_{q^2}} f(\Gamma_{a_{q^2}}) \right) \tag{2.3}$$

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

$${}_{a_i} f(\Gamma_{a_i}) = (f(a_i, b_{i_1}), \ldots, f(a_i, b_{i_q})).$$

This means that the codeword $(f(P_1), \ldots, f(P_n)) \in \mathcal{C}(\beta P_\infty, r)$ can be recovered by recovering each ${}_{a_i} f(\Gamma_{a_i})$ for $i \in [q^2]$.

The r-Hermitian codes over $\mathbb{F}_{q^{2l}}$ are nested, such that

$$\mathcal{C}(\beta P_\infty, 1) \subseteq \mathcal{C}(\beta P_\infty, 2) \subseteq \cdots \subseteq \mathcal{C}(\beta P_\infty, q).$$

For $r = 1$, we have that

$$\mathcal{C}(\beta P_\infty, 1) = \left\{ (f(a_1), \ldots, f(a_1), f(a_2), \ldots, f(a_2), \ldots, f(a_{q^2}), \ldots, f(a_{q^2})) : f \in \mathcal{L}(\beta P_\infty, 1) \right\},$$

where $\left\{a_1, \ldots, a_{q^2}\right\}$ are all the elements of $\mathbb{F}_{q^2}$; that is, $\mathcal{C}(\beta P_\infty, 1)$ is a kind of repetition Reed-Solomon code over an extension field $\mathbb{F}_{q^{2l}}$ whose the evaluation set is the base field $\mathbb{F}_{q^2}$. Meanwhile, for $r = q$, $\mathcal{C}(\beta P_\infty, q)$ is the constant extension code to $\mathbb{F}_{q^{2l}}$ of the one-point Hermitian code $C_{\mathcal{L}}(D, \beta P_\infty)$.

Remark 2. *Note that $\mathcal{C}(\beta P_\infty, r)$ is a code of length q^3 over $\mathbb{F}_{q^{2l}}$ whereas the codes considered in [12] are of length q^2 over $\mathbb{F}_{q^2}$; said differently, an r-Hermitian code of length q^3 is constructed over an alphabet of size q^{2l} whereas the codes of length q^3 considered in [12] employ a field of size q^{3l}. Both of these families of codes are shorter than Reed-Solomon codes over the same fields. However, they allow for fractional decoding (as proven in [12] and below for the r-Hermitian codes) whereas Reed-Solomon codes of length q over a field of size q do not.*

Proposition 3. *Let $r, l \in \mathbb{Z}, 1 \leq r \leq q$. The r-Hermitian code $\mathcal{C}(\beta P_\infty, r)$ is a $\mathbb{F}_{q^{2l}}$-linear code over $\mathbb{F}_{q^{2l}}$ of dimension given by*

$$\dim \mathcal{C}(\beta P_\infty, r) = \dim \mathcal{C}(\beta P_\infty) - \sum_{j=r}^{q-1} \left\lfloor \frac{\beta - j(q+1)}{q} \right\rfloor - q + r,$$

where $\mathcal{C}(\beta P_\infty) \subseteq \mathbb{F}_{q^2}^n$ is the one-point Hermitian code over $\mathbb{F}_{q^2}$.

Proof. Note that

$$\begin{aligned}
\dim \mathcal{C}(\beta P_\infty, r) &= |\{iq + j(q+1) : 0 \leq j \leq r-1; iq + j(q+1) \leq \beta\}| \\
&= \dim \mathcal{C}_l(\beta P_\infty) - |\{iq + j(q+1) : r \leq j \leq q-1; iq + j(q+1) \leq \beta\}| \\
&= \dim \mathcal{C}(\beta P_\infty) - |\{iq + j(q+1) : r \leq j \leq q-1; iq + j(q+1) \leq \beta\}| \\
&= \dim \mathcal{C}(\beta P_\infty) - \sum_{j=r}^{q-1} \left\lfloor \frac{\beta - j(q+1)}{q} \right\rfloor - q + r.
\end{aligned}$$

□

3 The fractional decoding problem

In this section, we introduce the fractional decoding problem. Then, as an example and to set the notation for more substantial results in Section 4, we consider fractional decoding of r-Hermitian codes via Reed-Solomon codes.

3.1 Preliminaries

Given an (n, k, l) array code $\mathcal{C}$ over a finite field $\mathbb{F}_q$, we may consider $\mathcal{C}$ as a code over the alphabet $\mathbb{F}_q^l$ and then one error amounts to an incorrect column C_i. Then correcting up to t errors means correcting any combination of errors $E = (E_1, \ldots, E_n)$ in $\left(\mathbb{F}_q^l\right)^n$ with Hamming weight $\omega(E) := |\{i : E_i \neq 0\}| \leq t$, where the received word is the matrix $R = C + E$. Note that the Hamming weight of a matrix counts the number of nonzero columns not the number of nonzero entries.

Motivated by applications in distributed storage, Tamo, Barg, and Ye [12], assume that each coordinate is stored on a separate node in the system and introduced the concept of fractional decoding where error correction by maximum distance separable codes based on part of the received word is considered. The idea of fractional decoding is that the decoder is allowed to download an α-proportion of each received word's coordinates. Below we will formally describe the fractional decoding problem.

Consider an (n, k, l) array code $\mathcal{C}$ over the field $\mathbb{F}_q$. The code $\mathcal{C}$ can correct up to t errors from an α-proportion of (the nl received) symbols of $\mathbb{F}_q$ if for each $i \in [n]$ there exists a function

$$f_i : \mathbb{F}_q^l \longrightarrow \mathbb{F}_q^{\alpha_i l} \quad \text{with} \quad \sum_{i=1}^{n} \alpha_i \leq n\alpha$$

and a function

$$g : \mathbb{F}_q^{(\sum_{i=1}^n \alpha_i) l} \longrightarrow \mathbb{F}_q^{nl}$$

such that for any codeword $(C_1, \ldots, C_n) \in \mathcal{C}$ and any error vector $E = (E_1, \ldots, E_n) \in \left(\mathbb{F}_q^l\right)^n$ of Hamming weight $\omega(E) \leq t$,

$$g(f_1(C_1 + E_1), f_2(C_2 + E_2), \ldots, f_n(C_n + E_n)) = (C_1, C_2, \ldots, C_n).$$

The α-decoding radius $r_\alpha(\mathcal{C})$ is the maximum number of errors that the code $\mathcal{C}$ can correct from an α-proportion of nl symbols of $\mathbb{F}_q$. The α-decoding radius of (n, k) codes is

$$r_\alpha(n, k) = \max_{\mathcal{C} \in \mathcal{M}_{n,k}} r_\alpha(\mathcal{C}),$$

where $\mathcal{M}_{n,k}$ is the set of all (n,k) codes.

Since the information content of a codeword $C \in \mathcal{C}$ is kl symbols of the field $\mathbb{F}_q$, the inequality $\alpha \geq \frac{k}{n}$ forms a necessary condition for decoding, even without errors. Hence, $r_\alpha(\mathcal{C}) > 0$ if and only if $\alpha \geq \frac{k}{n}$. This condition is assumed throughout the fractional decoding problem. For any $k \leq n$ and $\frac{k}{n} \leq \alpha \leq 1$ we have the following naive bound:

$$r_\alpha(n,k) \geq \left\lfloor \frac{\alpha n - k}{2} \right\rfloor. \tag{3.1}$$

Notice that $\alpha = 1$ is the standard decoding problem. Consequently, the goal of fractional decoding is to study error correction for α in the range $\frac{k}{n} \leq \alpha < 1$. Combining (3.1) with a result of [12], we see that the α-decoding radius of a (n,k) codes satisfies

$$\left\lfloor \frac{\alpha n - k}{2} \right\rfloor \leq r_\alpha(n,k) \leq \tau_\alpha := \left\lfloor \frac{n - \frac{k}{\alpha}}{2} \right\rfloor = \frac{1}{\alpha} \left\lfloor \frac{\alpha n - k}{2} \right\rfloor$$

where the upper bound $\frac{1}{\alpha}$ times the naive bound (3.1). A linear code $\mathcal{C}$ with α-decoding radius $r_\alpha(\mathcal{C}) = \tau_\alpha$ is said to have optimal α-decoding radius.

3.2 A basic fractional decoding algorithm for r-Hermitian codes

We begin by describing objects which support fractional decoding of r-Hermitian codes by harnessing fractional decoding of Reed-Solomon codes. In doing so, it is sometimes convenient to use indices in the set $[m]_0 := \{0, \ldots, m-1\}$ for an integer m. This subsection should be viewed as establishing the notation and a foundation to be used in the later, more powerful fractional decoding algorithms for r-Hermitian codes. There are some ideas similar to those in [8].

Given m pairwise disjoint sets $A_0, \ldots, A_{m-1} \subseteq \mathbb{F}_{q^2}$, define the annihilator polynomial of the set A_j, $j \in [m]_0$, to be

$$p_j(x) = \prod_{\omega \in A_j} (x - \omega) \in \mathbb{F}_{q^2}[x].$$

Note that $\deg p_j(x) = |A_j|$, $\forall j \in [m]_0$. Consider $F = \mathbb{F}_{q^{2l}}$ as an extension of $B = \mathbb{F}_{q^2}$ of degree l. Recall that the field trace of $\beta \in \mathbb{F}_{q^{2l}}$ relative to this extension is

$$tr_{F/B}(\beta) = \beta + \beta^{q^2} + \cdots + \beta^{q^{2(l-1)}} \in \mathbb{F}_{q^2}.$$

Let $\{\zeta_0, \zeta_1, \ldots, \zeta_{l-1}\}$ be a basis of F over B, and let $\{\nu_0, \nu_1, \ldots, \nu_{l-1}\}$ be its trace dual basis, meaning $tr_{F/B}(\zeta_s \nu_j) = \delta_{s,j}$ for all $s, j \in [l]_0$. Then

$$\beta = \sum_{s=0}^{l-1} tr_{F/B}(\zeta_s \beta) \nu_s.$$

In other words, any element β in F can be calculated from its l projections $\left\{tr_{F/B}(\zeta_s \beta)\right\}_{s=0}^{l-1}$ on B.

Definition 4. *Given a polynomial $h(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_0 \in \mathbb{F}_{q^{2l}}[x]$ and m pairwise disjoint subsets $A_0, \ldots, A_{m-1} \subseteq \mathbb{F}_{q^2}$. Define*

$$T_j(h)(x) = h_{l-m+j}(x)(p_j(x))^{(l-m)} + \sum_{u=0}^{l-m-1} h_u(x)(p_j(x))^u$$

for all $j \in [m]_0$, where

$$h_s(x) := tr(\zeta_s a_{k-1})x^{k-1} + tr(\zeta_s a_{k-2})x^{k-2} + \cdots + tr(\zeta_s a_0) \in \mathbb{F}_{q^2}[x].$$

For $f(x,y) \in \mathbb{F}_{q^{2l}}[x,y]$ given by

$$f(x,y) = \sum_{j=0}^{r-1} \sum_{i=0}^{s_j} a_{ij} x^i y^j \in \mathbb{F}_{q^{2l}}[x,y] \tag{3.2}$$

and $a \in \mathbb{F}_{q^{2l}}$, let

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

Furthermore, set

$$P_a^j(f) := T_j({}_af).$$

Lemma 5. *Let*

$$f(x,y) = \sum_{j=0}^{r-1} \sum_{i=0}^{s_j} a_{ij} x^i y^j \in \mathbb{F}_{q^{2l}}[x,y],$$

$a \in \mathbb{F}_{q^{2l}}$ *and* $A_0, \ldots, A_{m-1} \subseteq \mathbb{F}_{q^2}$ *be* m *pairwise disjoint subsets. Then,*

$$\deg P_a^j(f) \leq |A_j|(l-m) + r - 1 \text{ for } j \in [m]_0.$$

Moreover, if $\{(a,b_1),(a,b_2),\ldots,(a,b_n)\} \subseteq \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ *and* $B_a = \{b_1,\ldots,b_n\}$*, then*

$$P_a^j(f)(B_a) = \left(P_a^j(f)(b_1), P_a^j(f)(b_2), \ldots, P_a^j(f)(b_n)\right) \in \mathcal{RS}^{(q^2,1)}\left[n, k_j\right],$$

where $k_j = r + |A_j|(l-m)$ *and evaluation set* $B_a \subseteq \mathbb{F}_{q^2}$*. Meaning it is a codeword of a Reed-Solomon code over* $\mathbb{F}_{q^2}$*.*

Proof. Note that

$$\deg P_a^j(f)(y) = \max\left\{\deg\ {}_af_{l-m+j}(y)(p_j(y))^{(l-m)}, \deg \sum_{u=0}^{l-m-1}\ {}_af_u(y)(p_j(y))^u\right\}.$$

In addition,

$$\begin{aligned}\deg\ {}_af_{l-m+j}(y)(p_j(y))^{(l-m)} &= \deg\ {}_af_{l-m+j}(y) + \deg(p_j(y))(l-m)\\ &= r - 1 + |A_j|(l-m)\end{aligned}$$

and

$$\begin{aligned}\deg \sum_{u=0}^{l-m-1}\ {}_af_u(y)(p_j(y))^u &\leq \deg\ {}_af_{l-m-1}(y)(p_j(y))^{l-m-1}\\ &= r - 1 + |A_j|(l-m-1)\\ &\leq r - 1 + |A_j|(l-m),\end{aligned}$$

proving that $\deg P_a^j(f)(y) \leq |A_j|(l-m) + r - 1$.

Now, we must check that $P_a^j(f)(B_a) \in \mathbb{F}_{q^2}^n$. By definition, $P_a^j(f)(B_a) = (P_a^j(f)(b_1), \ldots, P_a^j(f)(b_n))$, so we just need to prove that $P_a^j(f)(b_i) \in \mathbb{F}_{q^2}$ for all $i \in [n]$. For any $j \in [m]_0$, we have

$$P_a^j(f)(b_i) =_a f_{l-m+j}(b_i)(p_j(b_i))^{(l-m)} + \sum_{u=0}^{l-m-1}\ {}_af_u(b_i)(p_j(b_i))^u. \tag{3.3}$$

It is clear that $P_a^j(f)(b_i) \in \mathbb{F}_{q^2}$ for all $i \in [n]$ since ${}_af_u(y), p_j(y) \in \mathbb{F}_{q^2}[y]$ and $b_i \in \mathbb{F}_{q^2}$, proving that $P_a^j(f)(B_a)$ is a codeword of the $\mathcal{RS}^{(q^2,1)}\left[n,k_j\right]$ code over $\mathbb{F}_{q^2}$ with evaluation set $B_a \subseteq \mathbb{F}_{q^2}$. □

Theorem 6. *Let*

$$f(x,y)=\sum_{j=0}^{r-1}\sum_{i=0}^{s_j}a_{ij}x^iy^j\in\mathbb{F}_{q^{2l}}[x,y],$$

$a\in\mathbb{F}_{q^2}$ *and* $A_0,\ldots,A_{m-1}\subseteq\mathbb{F}_{q^2}$ *be* m *pairwise disjoint subsets. If* $\sum_{j=0}^{m-1}|A_j|\geq r$*, then* $\{{}_af_s(y):s\in[l]_0\}$ *can be recovered from* $\{P_a^j(f)(y):j\in[m]_0\}$*. Consequently,* ${}_af(y)$ *can be recovered from* $\{P_a^j(f)(y):j\in[m]_0\}$*.*

Proof. Note that $P_a^j(f)(\omega)={}_af_0(\omega)$ for all $\omega\in A_j$; of course, we can rewrite $P_a^j(f)(y)$ as

$$\begin{aligned}P_a^j(f)(y) &= {}_af_{l-m+j}(y)(p_j(y))^{(l-m)}+\sum_{u=0}^{l-m-1}{}_af_u(y)(p_j(y))^u\\ &= {}_af_{l-m+j}(y)(p_j(y))^{(l-m)}+{}_af_0(y)(p_j(y))^0+\sum_{u=1}^{l-m-1}{}_af_u(y)(p_j(y))^u.\end{aligned}$$

Hence, $P_a^j(f)(\omega)={}_af_0(\omega)$ for all $\omega\in A_j$. Since we know the evaluations of ${}_af_0(y)$ at all the points of $\cup_{j=0}^{m-1}A_j$ and $\sum_{j=0}^{m-1}|A_j|\geq r\geq\deg\,{}_af_0(y)$, the ${}_af_0(y)$ can be recovered. Now from ${}_af_0(y)$ and $\{P_a^j(f)(y)\}_{j=0}^{m-1}$, we can calculate the polynomials

$$\begin{aligned}(P_a^j)^{(1)}(f)(y) &= \frac{P_a^j(f)(y)-{}_af_0(y)}{p_j(y)}\\ &= {}_af_{l-m+j}(y)(p_j(y))^{(l-m-1)}+{}_af_1(y)+\sum_{u=2}^{l-m-1}{}_af_u(y)(p_j(y))^{(u-1)}.\end{aligned}$$

Thus, $(P_a^j)^{(1)}(f)(\omega)={}_af_1(\omega)$ for all $\omega\in A_j$, and again, we know the evaluation of ${}_af_1(y)$ at all points of $\cup_{j=0}^{m-1}A_j$. Thus, we can recover ${}_af_1(y)$. From ${}_af_0(y)$,${}_a\,f_1(y)$ and $\{P_a^j(f)(y)\}_{j=0}^{m-1}$ we can calculate the polynomials

$$(P_a^j)^{(2)}(f)(y)=\frac{(P_a^j)^{(1)}(f)(y)-{}_af_1(y)}{p_j(y)}.$$

Since $(P_a^j)^{(2)}(f)(\omega)={}_af_2(\omega)$ for all $\omega\in A_j$, by the previous argument we can recover ${}_af_2(y)$. Generally, the polynomials $\{{}_af_{l-m+j}(y)\}_{j=0}^{m-1}$ can be recovered by

$${}_af_{l-m+j}(y)=\frac{P_a^j(f)(y)-\sum_{u=0}^{l-m-1}{}_af_u(y)(p_j(y))^u}{(p_j(y))^{(l-m)}}.$$

This shows that we can recover the polynomials $\{{}_af_j(y)\}_{j=0}^{m-1}$ from the polynomials $\{P_a^j(f)(y)\}_{j=0}^{m-1}$ and consequently recover ${}_af(y)$. □

The next proposition gives the relationship between the number of errors in coordinates corresponding to ${}_{a_i}f(\Gamma_{a_i})$ and the impact on the codewords $P_{a_i}^j(f)(\Gamma_{a_i})$ of Lemma 5.

Proposition 7. *Let* $\mathcal{C}(\beta P_\infty,r)$ *be an* r*-Hermitian code over* $\mathbb{F}_{q^{2l}}$ *and* $({}_{a_1}f(\Gamma_{a_1}),\ldots,{}_{a_{q^2}}f(\Gamma_{a_{q^2}}))$ *be a codeword as in (2.3) transmitted over a noisy channel. Assume that*

$$h:=({}_{a_1}h(\Gamma_{a_1}),\ldots,{}_{a_{q^2}}h(\Gamma_{a_{q^2}}))=({}_{a_1}f(\Gamma_{a_1}),\ldots,{}_{a_{q^2}}f(\Gamma_{a_{q^2}}))+({}_{a_1}e(\Gamma_{a_1}),\ldots,{}_{a_{q^2}}e(\Gamma_{a_{q^2}}))$$

is received. If ${}_{a_i}e(\Gamma_{a_i})=(e_1^i,e_2^i,\ldots,e_q^i)$ *has* t_i *nonzero entries* $e_{s_1}^i,e_{s_2}^i,\ldots,e_{s_{t_i}}^i$*, then* $P_{a_i}^j(h)(\Gamma_{a_i})$ *is a corrupted codeword of the* $\mathcal{RS}^{(q^2,1)}\,[q,r+|A_{ij}|(l-m)]$ *code with evaluation set* $\Gamma_{a_i}\subseteq\mathbb{F}_{q^2}$*. Moreover,* $P_{a_i}^j(h)(\Gamma_{a_i})$ *has most* t_i *errors at the positions* $s_1,s_2,\ldots,s_{t_i}$*.*

Proof. Note that $P_{a_i}^j(h)(\Gamma_{a_i})=P_{a_i}^j(f)(\Gamma_{a_i})+P_{a_i}^j(e)(\Gamma_{a_i})$. Clearly, if $e_u^i=0$ that is $u\notin\{s_1,\ldots,s_{t_i}\}$, then the respective coordinate in $P_{a_i}^j(e)(\Gamma_{a_i})$ is zero. If $u\in\{s_1,\ldots,s_{t_i}\}$ then the respective coordinate in $P_{a_i}^j(e)(\Gamma_{a_i})$ may be nonzero, so $P_{a_i}^j(h)(\Gamma_{a_i})$ has at most t_i errors. □

Now we are set to describe the fractional decoding procedure. Let $\mathcal{C}(\beta P_\infty, r)$ be an r-Hermitian code over $\mathbb{F}_{q^{2l}}$ and $\alpha = \frac{m}{l} < 1$, where m is a positive integer with $m|r$. For each $i \in [q^2]$, let $A_{i0}, A_{i1}, \ldots, A_{i(m-1)} \subseteq \mathbb{F}_{q^2}$ be m pairwise disjoint subsets of cardinality $\frac{r}{m}$ such that

$$\Gamma_{a_i} \subseteq \bigcup_{j=0}^{m-1} A_{ij} \subseteq \mathbb{F}_{q^2} \text{ and } \sum_{j=0}^{m-1} |A_{ij}| \geq r.$$

Remember that any codeword $(f(P_1), \ldots, f(P_{q^3})) \in \mathcal{C}(\beta P_\infty, r)$ can be viewed as

$$({}_{a_1}f(\Gamma_{a_1}), {}_{a_2}f(\Gamma_{a_2}), \ldots, {}_{a_{q^2}}f(\Gamma_{a_{q^2}})).$$

Since $|A_{ij}| = \frac{r}{m}$ and $\alpha = \frac{m}{l}$, $r + |A_{ij}|(l-m) = \frac{r}{\alpha}$. Hence, Lemma 5 implies that $P^j_{a_i}(f)(\Gamma_{a_i}) \in \mathcal{RS}^{(q^2,1)}\left[q, \frac{r}{\alpha}\right]$ and $\{P^j_{a_i}(f)(y) : j \in [m]_0\}$ can be recovered as long as there are no more than $\left\lfloor \frac{q-\frac{r}{\alpha}}{2} \right\rfloor$ errors in the received vector. Finally, by Theorem 6, the ${}_{a_i}f(y)$ can be recovered from $\{P^j_{a_i}(f)(y) : j \in [m]_0\}$. It remains to determine f. Notice that the number of terms of f is at most

$$\begin{aligned} \sum_{j=0}^{r-1} \sum_{i=0}^{s_j} 1 &\leq \alpha q^3 + q - \frac{q+1}{q} \sum_{i=0}^{q-1} i \\ &= \alpha q^3 + q - \frac{q^2}{2} < \alpha q^3 < q^3. \end{aligned}$$

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

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

for all $b \in \Gamma_{a_i}$. As a result, f can be recovered from ${}_{a_i}f(y)$, $i \in [q^2]$. This decoding procedure is summarized in the Algorithm 1.

Algorithm 1: Fractional decoding of r-Hermitian code via Reed-Solomon codes

input: Received word $h := ({}_{a_1}h(\Gamma_{a_1}), \ldots, {}_{a_{q^2}}h(\Gamma_{a_{q^2}})) = ev(f) + e \in \mathcal{C}(\beta P_\infty, r)$ where $f \in \mathcal{L}(\beta P_\infty, r)$ as in (2.2) and $\alpha = \frac{m}{l} < 1, m|r$.
for: $i \in [q^2]$ and $j \in [m]_0$ **do**
Download the q^2 sets of vectors $\{P^j_{a_i}(h)(\Gamma_{a_i})\}$ as in Lemma 5.
For each set $\{P^j_{a_i}(h)(\Gamma_{a_i})\}$ apply any decoding algorithm of $\mathcal{RS}$ codes to recover the set $\{P^j_{a_i}(f)(\Gamma_{a_i})\}$ and apply Theorem 6 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
  $$({}_{a_i}a_i, {}_{a_i}f(b_{i_s})).$$
  Use the pairs of the field elements obtained in the previous step to determine $f \in \mathcal{L}(\beta P_\infty, r)$.
else
  decoding failure
output: $f \in \mathcal{L}(\beta P_\infty, r)$ or decoding failure.

If ${}_{a_i}e(\Gamma_{a_i}) = (e^i_1, e^i_2, \ldots, e^i_q)$ has t_i nonzero entries $e^i_{s_1}, e^i_{s_2}, \ldots, e^i_{s_{t_i}}$ and $t_i < \left\lfloor \frac{q-\frac{r}{\alpha}}{2} \right\rfloor$ for all $i \in [q^2]$, then we say that the errors are well distributed.

Theorem 8. *Algorithm 1 can correct* $\left\lfloor \frac{q-\frac{r}{\alpha}}{2} \right\rfloor$ *errors. Moreover, Algorithm 1 can correct* $q^2 \left\lfloor \frac{q-\frac{r}{\alpha}}{2} \right\rfloor$ *errors provided they are well distributed.*

Proof. Suppose that a codeword $({}_{a_1}f(\Gamma_{a_1}),{}_{a_2}f(\Gamma_{a_2}),\ldots,{}_{a_{q^2}}f(\Gamma_{a_{q^2}})) \in \mathcal{C}(\beta P_\infty, r)$ was transmitted over a noisy channel and that $({}_{a_1}h(\Gamma_{a_1}),{}_{a_2}h(\Gamma_{a_2}),\ldots,{}_{a_{q^2}}h(\Gamma_{a_{q^2}}))$ was received. Each ${}_{a_i}f(\Gamma_{a_i})$ can be recovered via Algorithm 1 if the corresponding received vector ${}_{a_i}h(\Gamma_{a_i})$ has no more than $\left\lfloor \frac{q-\frac{r}{\alpha}}{2} \right\rfloor$ errors. Hence, it is possible to recover the original codeword if it has no more than $\left\lfloor \frac{q-\frac{r}{\alpha}}{2} \right\rfloor$ errors. Moreover, if each ${}_{a_i}h(\Gamma_{a_i})$ has no more than $\left\lfloor \frac{q-\frac{r}{\alpha}}{2} \right\rfloor$ errors, then each ${}_{a_i}f(\Gamma_{a_i})$ can be recovered. Hence, in the case of well distributed errors, Algorithm 1 can correct up to $q^2 \left\lfloor \frac{q-\frac{r}{\alpha}}{2} \right\rfloor$ errors. □

Note that to correct at least one error we must have $q - \frac{r}{\alpha} \geq 2$ and this is true if and only if $\alpha \geq \frac{r}{q-2}$. That is, Algorithm 1 works for $\frac{r}{q-2} \leq \alpha = \frac{m}{l} < 1$. Moreover, given an $\alpha < 1$ there is a trade-off beteween r and the number of errors that we can correct by downloading an α-proportion of a corrupted codeword: The smaller r is, the greater the number of errors we can correct by downloading an α-proportion of the corrupted codeword. Of course, this is not surprising given that larger values of r give codes of larger dimensions.

In the next section, we will see better ways to address fractional decoding of r-Hermitian codes.

4 Improving the fractional error correcting capability

In this section, we present algorithms to perform fractional decoding of r-Hermitian codes over $\mathbb{F}_{q^{2l}}$ which result in improved bounds on the fractional decoding radius. Some necessary background is provided in Subsection 4.1. In Subsections 4.2 and 4.3, we employ techniques from collaborative decoding for interleaved Reed-Solomon codes to ensure fractional decoding of r-Hermitian codes. We note that this approach is different from collaborative decoding of interleaved Hermitian codes. Indeed, the codes considered in this paper are constructed from the Hermitian curve. They are subcodes of the constant extension code to $\mathbb{F}_{q^{2l}}$ of the traditional one-point Hermitian code but are not interleaved Hermitian codes.

4.1 Interleaved Reed-Solomon codes and collaborative decoding

An interleaved code of order m induced by codes $\mathcal{C}_0, \ldots, \mathcal{C}_{m-1} \subseteq \mathbb{F}_q^n$ is the array code

$$\mathcal{IC}(\mathcal{C}_0, \ldots, \mathcal{C}_{m-1}) = \left\{ \begin{bmatrix} c_{0,1} & c_{0,2} & \cdots & c_{0,n-1} & c_{0,n} \\ c_{1,1} & c_{1,2} & \cdots & c_{1,n-1} & c_{1,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{m-1,1} & c_{m-1,2} & \cdots & c_{m-1,n-1} & c_{m-1,n} \end{bmatrix} : \begin{array}{l} (c_{i,1}, \ldots, c_{i,n}) \in \mathcal{C}_i, \\ 0 \leq i \leq m-1 \end{array} \right\}.$$

Sometimes we write a codeword $C \in \mathcal{IC}(\mathcal{C}_0, \ldots, \mathcal{C}_{m-1})$ as

$$C = \begin{bmatrix} c^{(0)} \\ c^{(1)} \\ \vdots \\ c^{(m-1)} \end{bmatrix}, \text{ where } c^{(i)} \in \mathcal{C}_i.$$

In particular, when the underlying codes are Reed-Solomon codes, the resulting interleaved code is said to be an interleaved Reed-Solomon code. More formally, it can be defined as follows.

Let $\mathcal{L} = \{\omega_1, \ldots, \omega_n\} \subseteq \mathbb{F}_q$ and $\mathcal{K} = \{k_0, k_1, \ldots, k_{m-1}\} \subseteq \mathbb{Z}^+$ where $k_j < n < q$ for any $0 \leq j \leq m-1$. An interleaved Reed-Solomon code $\mathcal{IRS}(q, n, \mathcal{K}, m)$ of order m is given by

$$\mathcal{IRS}(q, n, \mathcal{K}, m) = \left\{ \begin{bmatrix} f_0(\mathcal{L}) \\ f_1(\mathcal{L}) \\ \vdots \\ f_{m-1}(\mathcal{L}) \end{bmatrix} : f_j(x) \in \mathbb{F}_q[x], \deg(f_j) \leq k_j - 1 \right\}$$

where $f(\mathcal{L}) := (f(\omega_1), \ldots, f(\omega_n))$. The codewords $f_j(\mathcal{L}) \in \mathcal{RS}^{(q,1)}[n, k_j]$ are called elementary codewords of the $\mathcal{IRS}(q, n, \mathcal{K}, m)$ code. If the dimensions $k_j = k$ for all $j \in [m]_0$, the interleaved Reed-Solomon code is called a *homogeneous interleaved Reed-Solomon code* and is denoted by $\mathcal{IRS}(q, n, k, m)$. Otherwise, it is said to be a *heterogeneous interleaved Reed-Solomon code*.

The most common procedure to decode an interleaved code is to decode each row codeword $c^{(i)} \in \mathcal{C}_i$ separately. Using this decoding process, the maximum number of column errors that can be corrected in an interleaved code $\mathcal{IC}(\mathcal{C}_0, \ldots, \mathcal{C}_{m-1})$ is upper bounded by $\left\lfloor \frac{n - \max\{\dim(\mathcal{C}_i) : i \in [m]_0\}}{2} \right\rfloor$. In particular, for an interleaved Reed-Solomon code $\mathcal{IRS}(q, n, \mathcal{K}, m)$ the maximum number of column errors that can be corrected is $\left\lfloor \frac{n - \max\{k_0, \ldots, k_{m-1}\}}{2} \right\rfloor$.

Schmidt, Sidorenko, and Bossert introduced the concept of collaborative decoding for interleaved Reed-Solomon codes [11]. This decoder is based on the fact that the errors occur in the same positions of each elementary codeword of the interleaved Reed-Solomon code. We summarize some key results from [11] in preparation for applying them to r-Hermitian codes.

Consider a received word $R = C + E$ where $C \in \mathcal{IRS}(q, n, \mathcal{K}, m)$ and $E = (E_1, \ldots, E_n)$ denotes an error vector with t erroneous columns, meaning, $w(E) := |\{i : E_i \neq 0\}| = t$. The m elementary codewords of the interleaved Reed-Solomon code are affected by m elementary error words $e^{(0)}, e^{(1)}, \ldots, e^{(m-1)}$ of weight $w_H(e^{(j)}) = t_j \leq t$. Let $\mathcal{E}^{(j)}$ denote the set of error positions for the j-th elementary received word $r^{(j)}$. Since we are considering column errors, the union of the m sets of error positions $\mathcal{E} = \mathcal{E}^{(0)} \cup \mathcal{E}^{(1)} \cup \ldots \cup \mathcal{E}^{(m-1)}$ is a subset of $[n] := \{1, \ldots, n\}$ with cardinality $|\mathcal{E}| = t$.

Assuming that the codewords of the interleaved Reed-Solomon code are transmitted over a q^m-ary channel, the first step of collaborative decoding is to calculate the m syndrome polynomials $S^{(0)}(x), \ldots, S^{(m-1)}(x) \in \mathbb{F}_q[x]$ of degree less than $n - k_j$ where the j-th syndrome polynomial is

$$S^{(j)}(x) = \sum_{i=1}^{n-k_j} S_i^{(j)} x^{i-1}$$

with coefficients:

$$S_i^{(j)} = r^{(j)}(\omega_i^{k_j}) = \sum_{h=1}^{n} r_h^{(j)} \omega_i^{k_j(h-1)}$$

for all $i \in [n - k_j]$ and $j \in [m]_0$.

The Shift-Register Synthesis Algorithm [10, Algorithm 3] applied to the syndromes $S^{(0)}, \ldots, S^{(m-1)}$ yields a polynomial $\Lambda(x) \in \mathbb{F}_q[x]$ with $\Lambda(\omega_i^{-1}) = 0$ for all $i \in \mathcal{E}$. We may assume that this polynomial is normalized so that it is monic: $\Lambda(x) = \Lambda_1 + \Lambda_2 x + \cdots + \lambda_t x^{t-1} + x^t$. As in the classical case, these syndromes are used to form a linear system of equations $S\Lambda = V$,

$$\begin{bmatrix} S^{(0)} \\ S^{(1)} \\ \vdots \\ S^{(m-1)} \end{bmatrix} \begin{bmatrix} \Lambda_1 \\ \Lambda_2 \\ \vdots \\ \Lambda_t \end{bmatrix} = \begin{bmatrix} V^{(0)} \\ V^{(1)} \\ \vdots \\ V^{(m-1)} \end{bmatrix}, \tag{4.1}$$

where each submatrix $S^{(j)}$ is a $(n - k_j - t) \times t$ matrix and each $V^{(j)}$ is a column vector of length $n - k_j - t$:

$$S^{(j)} = \begin{bmatrix} S_1^{(j)} & S_2^{(j)} & \cdots & S_t^{(j)} \\ S_2^{(j)} & S_3^{(j)} & \cdots & S_{t+1}^{(j)} \\ \vdots & \vdots & \ddots & \vdots \\ S_{n-k_j-t}^{(j)} & S_{n-k_j-t+1}^{(j)} & \cdots & S_{n-k_j-1}^{(j)} \end{bmatrix}, V^{(j)} = \begin{bmatrix} -S_{t+1}^{(j)} \\ -S_{t+2}^{(j)} \\ \vdots \\ -S_{n-k_j}^{(j)} \end{bmatrix}.$$

The system of equations (4.1) has $\sum_{j=0}^{m-1} (n - k_j - t)$ equations and t unknowns. In order to guarantee unambiguous decoding, the number of linearly independent equations has to be greater than or equal to the number of unknowns.

Under the assumption that all equations in (4.1) are linearly independent,

$$\sum_{j=0}^{m-1}(n-k_j-t)\geq t$$

which can be rewritten as

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

The number

$$\tau_{IRS}:=\frac{m}{m+1}\left(n-\frac{1}{m}\sum_{j=0}^{m-1}k_j\right)$$

is called the joint-error-correcting capability of the interleaved Reed-Solomon code. However, there is a certain probability that some of the equations (4.1) are linearly dependent. In this case, there is no unique solution to the system of equations, and *decoding failure* is declared.

The collaborative decoding algorithm from [11] is outlined in Algorithm 2. It can correct t errors where $t\leq\tau_{\mathcal{IRS}}$ with a failure probability

$$P_F(t)\leq\left(\frac{q^m-\frac{1}{q}}{q^m-1}\right)^t\frac{q^{-(m+1)(\tau_{\mathcal{IRS}}-t)}}{q-1}.$$

Algorithm 2: Collaborative $\mathcal{IRS}$ Decoder

input: Received word $R=\begin{bmatrix}r^{(0)}\\ r^{(1)}\\ \vdots\\ r^{(m-1)}\end{bmatrix}$. Calculate syndromes $S^{(0)},\ldots,S^{(m-1)}$.

Compute t and $\Lambda(x)$ by Algorithm 4 in [10].

if $t<\tau_{\mathcal{IRS}}$ **and** $\Lambda(x)$ is t-valid **then**

  for each j from 0 to $m-1$ **do**

  evaluate errors, and calculate $e^{(j)}$

  calculate $\hat{c}^{(j)}=r^{(j)}+e^{(j)}$

else

  decoding failure

output: $C\in\mathcal{IRS}(q,n,\mathcal{K},m)$ or decoding failure

4.2 Fractional decoding via homogeneous interleaved Reed-Solomon codes

Recall that Algorithm 1 downloads m symbols from each ${}_{a_i}h(\Gamma_{a_i})$, which is a corrupted codeword of $\mathcal{RS}^{(q^2,1)}\left[q,\frac{r}{\alpha}\right]$. Those m symbols can be arranged to form the following matrix

$$\pi_i(h)=\begin{bmatrix}P^0_{a_i}(h)(\Gamma_{a_i})\\ P^1_{a_i}(h)(\Gamma_{a_i})\\ \vdots\\ P^{m-1}_{a_i}(h)(\Gamma_{a_i})\end{bmatrix}\in\left(\mathbb{F}_{q^2}^m\right)^q;$$

that is, the downloaded symbols may be viewed as a codeword of a homogeneous interleaved Reed-Solomon code

$$\mathcal{IRS}\left(q^2,q,\frac{r}{\alpha},m\right)=\left\{\begin{bmatrix}f_0(\Gamma_{a_i})\\ f_1(\Gamma_{a_i})\\ \vdots\\ f_{m-1}(\Gamma_{a_i})\end{bmatrix}:\ f_j(x)\in\mathbb{F}_{q^2}[x],\deg(f_j)\leq\frac{r}{\alpha}-1\right\}.$$

We take this perspective and consider their projections.

Definition 9. *Let* $h = ({}_{a_1}h(\Gamma_{a_1}), {}_{a_2}h(\Gamma_{a_2}), \ldots, {}_{a_{q^2}}h(\Gamma_{a_{q^2}})) \in \mathbb{F}_{q^{2l}}^n$ *and* $P_{a_i}^j(h)$ *be as in Definition 4. Then the matrix* $\pi_i(h) \in \left(\mathbb{F}_{q^2}^m\right)^q$ *is called the* i*-th projection of* h *to a homogeneous interleaved Reed-Solomon code. Moreover, the matrix*

$$\pi(h) := \left[\pi_1(h) \mid \pi_2(h) \mid \cdots \mid \pi_{q^2}(h)\right] \in \left(\mathbb{F}_{q^2}^m\right)^n$$

is called the homogeneous virtual projection of h*.*

Now, Proposition 7 can be recast in this setting as follows, with a similar proof.

Proposition 10. *Let* $(f(P_1), f(P_2), \ldots, f(P_n)) \in \mathcal{C}(\beta P_\infty, r)$ *be a codeword as in (2.3) transmitted over a noisy channel. Assume that*

$$({}_{a_1}h(\Gamma_{a_1}), \ldots, {}_{a_{q^2}}h(\Gamma_{a_{q^2}})) = ({}_{a_1}f(\Gamma_{a_1}), \ldots, {}_{a_{q^2}}f(\Gamma_{a_{q^2}})) + ({}_{a_1}e(\Gamma_{a_1}), \ldots, {}_{a_{q^2}}e(\Gamma_{a_{q^2}}))$$

is received. If ${}_{a_i}e(\Gamma_{a_i}) = (e_1^i, e_2^i, \ldots, e_q^i)$ *has* t_i *nonzero entries* $e_{s_1}^i, e_{s_2}^i, \ldots, e_{s_{t_i}}^i$*, then* $\pi_i(h)$ *is a corrupted codeword of the homogeneous* $\mathcal{IRS}(q^2, q, \frac{r}{\alpha}, m)$ *code with at most* t_i *erroneous columns at the positions* $s_1, s_2, \ldots, s_{t_i}$*.*

Due to Proposition 10, we can use collaborative decoding as in Algorithm 2 and Theorem 6 to recover ${}_{a_i}f$ from t_i errors with failure probability given by

$$P_F(t_i) \leq \left(\frac{q^{2m} - \frac{1}{q^2}}{q^{2m} - 1}\right)^{t_i} \frac{q^{-2(m+1)(\tau_\star - t_i)}}{q^2 - 1} \tag{4.2}$$

where $\tau_\star := \frac{m}{m+1}\left(q - \frac{r}{\alpha}\right)$ since

$$t_i \leq \frac{m}{m+1}\left(q - \frac{r}{\alpha}\right).$$

The resulting fractional decoding algorithm is outlined in Algorithm 3.

Algorithm 3: Fractional decoding of r-Hermitian code via virtual projection to a homogeneous interleaved Reed-Solomon code

input: Received word $h = ev(f) + e \in \mathcal{C}(\beta P_\infty, r)$ where $f \in \mathcal{L}(\beta P_\infty, r)$ as in (2.2) and $\alpha = \frac{m}{l} < 1, m|r$.

for: $i \in [q^2]$, and $j \in [m]_0$ **do**

Download the entries of the virtual projection $\pi(h) \in \left(\mathbb{F}_{q^2}^m\right)^q$.

For each submatrix $\pi_i(h)$ of $\pi(h)$ apply Algorithm 2 and Theorem 6 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

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

  Use the pairs of the field elements obtained in the previous step to determine $f \in \mathcal{L}(\beta P_\infty, r)$.

else

  decoding failure

output: $f \in \mathcal{L}(\beta P_\infty, r)$ or decoding failure.

Recall that Algorithm 1 corrects up to $t \leq \frac{1}{2}\left(q - \frac{r}{\alpha}\right)$ errors. The next result captures the improvement of the perspective provided by interleaved codes.

Theorem 11. *Algorithm 3 corrects up to* $\frac{m}{m+1}\left(q - \frac{r}{\alpha}\right)$ *errors. Moreover, if the errors are well distributed, Algorithm 3 can correct up to* $q^2\frac{m}{m+1}\left(q - \frac{r}{\alpha}\right)$ *errors.*

Proof. Suppose that a codeword $f = ({}_{a_1}f(\Gamma_{a_1}), {}_{a_2}f(\Gamma_{a_2}), \ldots, {}_{a_{q^2}}f(\Gamma_{a_{q^2}})) \in \mathcal{C}(\beta P_\infty, r)$ is transmitted over a noisy channel and that $h = ({}_{a_1}h(\Gamma_{a_1}), {}_{a_2}h(\Gamma_{a_2}), \ldots, {}_{a_{q^2}}h(\Gamma_{a_{q^2}}))$ is received. Each ${}_{a_i}f$ can be recovered with failure probability $P_F(t_i)$ via Algorithm 3 if the corresponding i-th projection $\pi_i(h)$ has no more than t_i errors $t_i \leq \tau_\star$. So, it is always possible to recover the original codeword if it has no more than $\frac{m}{m+1}\left(q - \frac{r}{\alpha}\right)$ errors. Moreover, note that if the error positions in the received word are such that for each $i \in [q^2]$ the number of errors in the corresponding i-th projection $\pi_i(h)$ has no more than $t_i = \tau_\star$ errors, the original codeword can be recovered. Hence, in the case of well distributed errors, Algorithm 3 can correct up to $q^2\frac{m}{m+1}\left(q - \frac{r}{\alpha}\right)$ errors. □

As indicated by Theorem 11, Algorithm 3 improves the α-error correcting capability of Algorithm 1. Indeed,

$$\frac{m}{m+1}\left(q - \frac{r}{\alpha}\right) \geq \frac{1}{2}\left(q - \frac{r}{\alpha}\right)$$

for all $m \geq 1$.

4.3 Fractional decoding via heterogeneous interleaved Reed-Solomon codes

Next, we consider a slight modification of the operator T_j of Definition 4 that when coupled with an additional condition on the r-Hermitian code makes it possible to use collaborative decoding of heterogeneous interleaved Reed-Solomon codes to present a new fractional decoding algorithm.

Definition 12. *Given a polynomial $h(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_0 \in \mathbb{F}_{q^{2l}}[x]$ and m pairwise disjoint subsets $A_0, A_1, \ldots, A_{m-1} \subseteq \mathbb{F}_{q^2}$. For all $j \in [m]_0$, define*

$$R_j(h)(x) = h_{l-m+j}(x)(p_j(x))^{(l-m)(j+1)} + \sum_{u=0}^{l-m-1} h_u(x)(p_j(x))^{u(j+1)},$$

where

$$h_s(x) = tr(\zeta_s a_{k-1})x^{k-1} + tr(\zeta_s a_{k-2})x^{k-2} + \ldots + tr(\zeta_s a_0) \in \mathbb{F}_{q^2}[x].$$

For $f(x, y) \in \mathbb{F}_{q^{2l}}[x, y]$ as in (3.2), define

$$H_a^j(f)(y) := R_j({}_af(y)). \tag{4.3}$$

Using ideas similar to Lemma 5 and Theorem 6, one may verify the following results.

Lemma 13. *Consider*

$$f(x, y) = \sum_{j=0}^{r-1}\sum_{i=0}^{s_j} a_{ij}x^i y^j \in \mathbb{F}_{q^{2l}}[x, y],$$

$a \in \mathbb{F}_{q^{2l}}$ and m pairwise disjoint subsets $A_0, A_1, \ldots, A_{m-1} \subseteq \mathbb{F}_{q^2}$. Then

$$\deg H_a^j(f)(y) \leq |A_j|(l-m)(j+1) + r - 1.$$

Furthermore, if $\{(a, b_1), (a, b_2), \ldots, (a, b_n)\} \subseteq \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ and $B_a = \{b_1, \ldots, b_n\}$, then

$$H_a^j(f)(B_a) = (H_a^j(f)(b_1), H_a^j(f)(b_2), \ldots, H_a^j(f)(b_n))$$

is a codeword of the Reed-Solomon code

$$\mathcal{RS}^{(q^2,1)}\left[n, r + |A_j|(l-m)(j+1)\right].$$

Theorem 14. *Let*

$$f(x, y) = \sum_{j=0}^{r-1}\sum_{i=0}^{s_j} a_{ij}x^i y^j \in \mathbb{F}_{q^{2l}}[x, y],$$

$a \in \mathbb{F}_{q^2}$ and $A_0, \ldots, A_{m-1} \subseteq \mathbb{F}_{q^2}$ be m pairwise disjoint subsets. If $\sum_{j=0}^{m-1}|A_j| \geq r$, then $\{{}_af_s(y) : s \in [l]_0\}$ can be recovered from $\{H_a^j(f)(y) : j \in [m]_0\}$. Consequently, ${}_af(y)$ can be recovered from $\{H_a^j(f)(y) : j \in [m]_0\}$.

Next, we consider heterogeneous projections.

Definition 15. *Consider* $f = ({}_{a_1}f(\Gamma_{a_1}),{}_{a_2}f(\Gamma_{a_2}),\ldots,{}_{a_{q^2}}f(\Gamma_{a_{q^2}})) \in \mathcal{C}(\beta P_\infty, r)$. *For each* $i \in [q^2]$, *let* $A_{i,0},\ldots,A_{i,m-1}$ *be* m *pairwise disjoint subsets of* $\mathbb{F}_{q^2}$ *such that* $\sum_{j=0}^{m-1}|A_{i,j}| \geq r$. *The matrix*

$$\pi_i^\star(f) = \begin{bmatrix} H_{a_i}^0(f)(\Gamma_{a_i}) \\ H_{a_i}^1(f)(\Gamma_{a_i}) \\ \vdots \\ H_{a_i}^{m-1}(f)(\Gamma_{a_i}) \end{bmatrix} \in \left(\mathbb{F}_{q^2}^m\right)^q$$

is called the i*-th projection of* f *to a heterogeneous interleaved Reed-Solomon code.*

Further, the i*-th projection of* $\mathcal{C}(\beta P_\infty, r)$ *to a heterogeneous interleaved Reed-Solomon code is given by*

$$\pi_i^\star(\mathcal{C}) = \left\{\pi_i^\star(f) : f = ({}_{a_1}f(\Gamma_{a_1}),{}_{a_2}f(\Gamma_{a_2}),\ldots,{}_{a_{q^2}}f(\Gamma_{a_{q^2}})) \in \mathcal{C}(\beta P_\infty, r)\right\} \subseteq \left(\mathbb{F}_{q^2}^m\right)^q.$$

The heterogeneous virtual projection of $\mathcal{C}(\beta P_\infty, r)$ *is the array code* $\mathcal{C}_{P_{m/l}}^\star = \mathcal{C}_{P_{m/l}}^\star(q^2, n, m, \mathcal{K})$ *given by*

$$\mathcal{C}_{p_{m/l}}^\star := \left\{\pi^\star(f) = [\pi_1^\star(f)|\ldots|\pi_{q^2}^\star(f)] : ({}_{a_1}f(\Gamma_{a_1}),{}_{a_2}f(\Gamma_{a_2}),\ldots,{}_{a_{q^2}}f(\Gamma_{a_{q^2}})) \in \mathcal{C}(\beta P_\infty, r)\right\},$$

where $\mathcal{K} = \{r + |A_{i,j}|(l-m)(j+1), \forall j \in [m]_0\}$.

Assume that $({}_{a_1}f(\Gamma_{a_1}),{}_{a_2}f(\Gamma_{a_2}),\ldots,{}_{a_{q^2}}f(\Gamma_{a_{q^2}})) \in \mathcal{C}(\beta P_\infty, r)$ is transmitted over a noisy channel, which adds t errors in such a way that the word

$$h := ({}_{a_1}h(\Gamma_{a_1}),\ldots,{}_{a_{q^2}}h(\Gamma_{a_{q^2}})) = ({}_{a_1}f(\Gamma_{a_1}),\ldots,{}_{a_{q^2}}f(\Gamma_{a_{q^2}})) + ({}_{a_1}e(\Gamma_{a_1}),\ldots,{}_{a_{q^2}}e(\Gamma_{a_{q^2}}))$$

is observed at the channel output. Using the observed word h, we can calculate the q^2m polynomials $H_{a_i}^j(h)(y)$ and create the matrix

$$\pi^\star(h) = [\pi_1^\star(h)|\pi_2^\star(h)|\ldots|\pi_{q^2}^\star(h)].$$

The matrix $\pi^\star(h)$ can be considered as a corrupted received word of the heterogeneous virtual projection code $\mathcal{C}_{P_{m/l}}^\star(q^2, n, m, \mathcal{K})$ of $\mathcal{C}(\beta P_\infty, r)$. The next theorem shows how errors in $\mathcal{C}(\beta P_\infty, r)$ affect $\mathcal{C}_{P_{m/l}}^\star(q^2, n, m, \mathcal{K})$.

Proposition 16. *Let* $f = ({}_{a_1}f(\Gamma_{a_1}),{}_{a_2}f(\Gamma_{a_2}),\ldots,{}_{a_{q^2}}f(\Gamma_{a_{q^2}}))$ *be a codeword of an* r*-Hermitian code* $\mathcal{C}$ *transmitted over a noisy channel. Assume that*

$$h := ({}_{a_1}h(\Gamma_{a_1}),\ldots,{}_{a_{q^2}}h(\Gamma_{a_{q^2}})) = ({}_{a_1}f(\Gamma_{a_1}),\ldots,{}_{a_{q^2}}f(\Gamma_{a_{q^2}})) + ({}_{a_1}e(\Gamma_{a_1}),\ldots,{}_{a_{q^2}}e(\Gamma_{a_{q^2}}))$$

is received. If ${}_{a_i}e(\Gamma_{a_i}) = (e_{(i,1)}, e_{(i,2)},\ldots,e_{(i,q)})$ *has* t_i *nonzero entries* $e_{(i,s_1)},\ldots,e_{(i,s_{t_i})}$, *then* $\pi^\star(h)$ *is a corrupted codeword of the* $\mathcal{C}_{P_{m/l}}^\star(q^2, n, m, \mathcal{K})$ *code with at most* t_i *erroneous columns at positions* $(i, s_1),\ldots,(i, s_{t_i})$.

Proof. Note that $\pi_i^\star(h) = \pi_i^\star(f+e) = \pi_i^\star(f) + \pi_i^\star(e)$. Clearly, if $e_{(i,u)} = 0$, meaning $u \notin \{s_1,\ldots,s_{t_i}\}$, then the respective coordinate in $H_{a_i}^j(e)$ is zero. If $u \in \{s_1,\ldots,s_{t_i}\}$, then the respective coordinate in $H_{a_i}^j(e)$ may be nonzero. Hence, $\pi_i^\star(h)$ has at most t_i erroneous columns at positions $(i, s_1),\ldots,(i, s_{t_i})$. □

Next, we will provide a fractional decoding procedure an r-Hermitian code via its heterogeneous virtual projection.

Let $\mathcal{C}(\beta P_\infty, r)$ be an r-Hermitian code over $\mathbb{F}_{q^{2l}}$, $\alpha = \frac{m}{l} < 1$, where m is a positive integer such that $m|r$. For each $i \in [q^2]$, let $A_{i0}, A_{i1},\ldots,A_{i(m-1)} \subseteq \mathbb{F}_{q^2}$ be m pairwise disjoint subsets of same cardinality $\frac{r}{m}$, such that

$$\Gamma_{a_i} \subseteq \bigcup_{j=0}^{m-1} A_{ij} \subseteq \mathbb{F}_{q^2} \text{ and } \sum_{j=0}^{m-1}|A_{ij}| \geq r.$$

According to Theorem 14, ${}_{a_i}f(y)$ can be recovered from $\{H^j_{a_i}(f)(y) : j \in [m]_0\}$. By Lemma 13, $H^j_{a_i}(\Gamma_{a_i}) \in \mathcal{RS}^{(q^2,1)}\left[q, r+\frac{r}{m}(l-m)(j+1)\right] = \mathcal{RS}^{(q^2,1)}\left[q, r+\left(\frac{r}{\alpha}-r\right)(j+1)\right]$. Hence, the i-th virtual projection of f, $\pi^\star_i(f) \in \mathcal{IRS}\left(q^2, q, \mathcal{K}, m\right)$, where $\mathcal{K} = \left\{k_j = r+\left(\frac{r}{\alpha}-r\right)(j+1),\ j \in [m]_0\right\}$. Hence, we can recover $\pi^\star_i$ from $t_i \leq \tau^\star$ errors with failure probability

$$P_F(t_i) \leq \left(\frac{q^{2m}-\frac{1}{q^2}}{q^{2m}-1}\right)^{t_i} \frac{q^{-2(m+1)(\tau^\star-t_i)}}{q^2-1}$$

where

$$\tau^\star := \frac{1}{m+1}\left[mq - \frac{r}{\alpha}\binom{m+1}{2} + r\binom{m}{2}\right]$$

and consequently recover ${}_{a_i}f(y)$. It remains to determine f. Notice that the number of terms of f is at most

$$\begin{aligned}\textstyle\sum_{j=0}^{r-1}\sum_{i=0}^{k_j} 1 &\leq \alpha q^3 + q - \tfrac{q+1}{q}\textstyle\sum_{i=0}^{q-1} i \\ &= \alpha q^3 + q - \tfrac{q^2}{2} < \alpha q^3 < q^3.\end{aligned}$$

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

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

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

This decoding procedure is summarized in Algorithm 4.

Algorithm 4: Fractional decoding of r-Hermitian code via virtual projection to a heterogeneous interleaved Reed-Solomon code

---

input: Received word $h = ev(f) + e \in \mathcal{C}(\beta P_\infty, r)$ where $f \in \mathcal{L}(\beta P_\infty, r)$ as in (2.2) and $\alpha = \frac{m}{l} < 1$.
for: $i \in [q^2]$, and $j \in \underline{[m]}$ **do**
Download the entries of the virtual projetion $\pi^\star(h) \in \left(\mathbb{F}_{q^2}^m\right)^n$.
For each submatrix $\pi^\star_i(h)$ of $\pi^\star(h)$ apply Algorithm 2 and Theorem 14 to recover ${}_{a_i}f$.
if $\underline{{}_{a_i}f \text{ is successfully recovered for all } i \in [q^2]}$ **then**
  for each $s \in [q]$ **do**
  Calculate the points

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

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

Theorem 17. *Algorithm 4 can correct $\frac{1}{m+1}\left[mq - \frac{r}{\alpha}\binom{m+1}{2} + r\binom{m}{2}\right]$ errors. Moreover, Algorithm 4 can correct up to $\frac{q^2}{m+1}\left[mq - \frac{r}{\alpha}\binom{m+1}{2} + r\binom{m}{2}\right]$ errors if they are well distributed.*

Proof. Suppose that a codeword $({}_{a_1}f(\Gamma_{a_1}), {}_{a_2}f(\Gamma_{a_2}), \ldots, {}_{a_{q^2}}f(\Gamma_{a_{q^2}})) \in \mathcal{C}(\beta P_\infty, r)$ was transmitted over a noisy channel and that $({}_{a_1}h(\Gamma_{a_1}), {}_{a_2}h(\Gamma_{a_2}), \ldots, {}_{a_{q^2}}h(\Gamma_{a_{q^2}}))$ was received. Each ${}_{a_i}f$ can be recovered via Algorithm 4 with failure probability

$$P_F(t_i) \leq \left(\frac{q^{2m}-\frac{1}{q^2}}{q^{2m}-1}\right)^{t_i} \frac{q^{-2(m+1)(\tau^\star-t_i)}}{q^2-1}$$

if the corresponding i-th projection $\pi^\star_i(h)$ has no more than $t_i \leq \tau^\star$ errors. Hence, it is possible to recover the original codeword if no more than $\tau^\star$ errors have occurred. Moreover, note that if the error positions in the received word are such that for each $i \in [q^2]$ the number of errors in the corresponding i-th projection $\pi^\star_i(h)$ has no more than $\tau^\star$ errors, the original codeword will be recovered. Thus, in this situation, Algorithm 4 can correct $q^2\tau^\star$ errors. □

Next, we consider when Algorithm 4 provides an improvement over Algorithm 1 or Algorithm 3.

Proposition 18. *Consider the r-Hermitian code $\mathcal{C}(\beta P_\infty, r)$ over $\mathbb{F}_{q^{2l}}$, $\alpha = \frac{m}{l}$ such that $m|r$. Fractional decoding of $\mathcal{C}(\beta P_\infty, r)$ via virtual projection to heterogeneous interleaved Reed-Solomon codes (Algorithm 4) corrects more errors than via Reed-Solomon codes (Algorithm 1) if and only if*

$$\frac{r}{q} \leq \frac{\alpha}{(1-\alpha)(m+1)}.$$

Fractional decoding of $\mathcal{C}(\beta P_\infty, r)$ via heterogeneous interleaved Reed-Solomon codes (Algorithm 4) corrects more errors than via homogeneous interleaved Reed-Solomon codes (Algorithm 3) if and only if

$$m \geq \frac{1+\sqrt{1+4l}}{2}.$$

Proof. The proof follows from direct computation. First, it can be verified that

$$\tau^\star \geq \frac{q - \frac{r}{\alpha}}{2}$$

if and only if

$$\frac{r}{q} \leq \frac{\alpha}{(1-\alpha)m+1}.$$

Second, one may check that

$$\tau^\star \geq \frac{m}{m+1}\left(q - \frac{r}{\alpha}\right) = \tau_\star$$

if and only if

$$m \geq \frac{1+\sqrt{1+4l}}{2}.$$

□

5 Conclusion

In this paper, we define a family of codes, called r-Hermitian codes, and provide fractional decoding algorithms for them. Several approaches are provided, including via Reed-Solomon codes as well as via homogeneous and heterogeneous interleaved Reed-Solomon codes. Because the algorithms may output decoding failure if errors are concentrated in particular blocks, it is an interesting research problem to consider how other possible partitions of the evaluation points may support successful decoding.

References

[1] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran. Network coding for distributed storage systems. IEEE Transactions on Information Theory, 56(9):4539–4551, 2010.

[2] Y. Gao, Q. Yue, X. Huang, and J. Zhang. Hulls of generalized Reed-Solomon codes via Goppa codes and their applications to quantum codes. IEEE Transactions on Information Theory, 67(10):6619–6626, 2021.

[3] S. Ghemawat, H. Gobioff, and S.-T. Leung. The Google file system. In Proceedings of the 19th ACM Symposium on Operating Systems Principles, pages 20–43, Bolton Landing, NY, 2003.

[4] V. Guruswami and C. Xing. List decoding Reed-Solomon, algebraic-geometric, and Gabidulin subcodes up to the Singleton bound. In Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing, STOC 13, pages 843–852, New York, NY, USA, 2013. Association for Computing Machinery.

[5] C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, and S. Yekhanin. Erasure coding in Windows Azure storage. In Proceedings of the 2012 USENIX Conference on Annual Technical Conference, USENIX ATC'12, page 2, USA, 2012. USENIX Association.

[6] J. Kubiatowicz, D. Bindel, Y. Chen, S. Czerwinski, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Zhao. Oceanstore: An architecture for global-scale persistent storage. SIGPLAN Not., 35(11):190–201, 2000.

[7] H. H. Lopez and G. L. Matthews. Multivariate Goppa codes. IEEE Transactions on Information Theory, pages 1–1, 2022.

[8] G. L. Matthews, A. W. Murphy, and W. Santos. Fractional decoding of codes from Hermitian curves. In 2021 IEEE International Symposium on Information Theory (ISIT), pages 515–520, 2021.

[9] W. Santos. On fractional decoding of Reed-Solomon codes. In 2019 IEEE International Symposium on Information Theory (ISIT), pages 1552–1556, 2019.

[10] G. Schmidt and V. R. Sidorenko. Multi-sequence linear shift-register synthesis: The varying length case. In 2006 IEEE International Symposium on Information Theory, pages 1738–1742, 2006.

[11] G. Schmidt, V. R. Sidorenko, and M. Bossert. Collaborative decoding of interleaved Reed-Solomon codes and concatenated code designs. IEEE Transactions on Information Theory, 55(7):2991–3012, 2009.

[12] I. Tamo, M. Ye, and A. Barg. Fractional decoding: Error correction from partial information. In 2017 IEEE International Symposium on Information Theory (ISIT), pages 998–1002, 2017.