Error correction from partial information via norm-trace codes

Eduardo Camps-Moreno & Gretchen L. Matthews
Department of Mathematics
Virginia Tech
Blacksburg, VA, USA
Email: e.camps@vt.edu, gmatthews@vt.edu

Welington Santos
Department of Mathematics, Statistics,
& Computer Science
University of Wisconsin-Stout
Menomonie, WI, USA
Email: santosw@uwstout.edu

2024 IEEE International Symposium on Information Theory (ISIT) | 979-8-3503-8284-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISIT57864.2024.10619093

***Abstract*—In this paper, we consider using norm-trace codes over extension fields for error correction using partial information from received words. To do so, we define virtual projections of norm-trace codes and we implement a fractional decoding scheme. The scheme depends on a refined key equation tailored to the norm-trace code.**

***Index Terms*—algebraic geometry code, distributed storage, norm-trace curve, fractional decoding, partial information**

I. Introduction

Tamo, Ye, and Barg [16] introduced the fractional decoding problem, motivated by distributed storage systems in which there are limitations on the disk operation and on the amount of information transmitted for the purpose of decoding. They outlined the concept of error correction with partial information for codes defined over an extension field, focusing on maximum distance separable (MDS) codes. Fractional decoding seeks to consider codes defined over extension fields and algorithms for error correction that use fewer symbols than usual from the base field, thus operating using a restricted amount of information in the decoding process. In [15], Santos provided a connection between fractional decoding of Reed-Solomon codes, which can be considered as codes from the projective line, a curve of genus 0, and collaborative decoding of interleaved Reed-Solomon codes. Later in [13], [14], an algorithm is given for fractional decoding of r-Hermitian codes, which are constant field extensions of subcodes of the one-point Hermitian codes.

In this paper, we present a fractional decoding approach for one-point codes from the norm-trace curves where the evaluation points have coordinates that lie in a proper subfield (as done by Guruswami and Xing [6] and Gao, Yue, Huang, and Zhang [3], among others). The codes considered in this paper and those in [16] have lengths q^{2r-1}, over alphabet sizes of q^{rl} and $q^{(2r-1)l}$ respectively. While they are shorter than Reed-Solomon codes over the same alphabets, they allow for fractional decoding with $\alpha < 1$, whereas Reed-Solomon codes themselves do not. Moreover, norm-trace codes with $r > 2$ can have better relative parameters than Hermitian codes and give a step in the direction of fractional decoding for more general families of curves.

The first and second authors are partially supported by NSF DMS-2201075 and the Commonwealth Cyber Initiative.

This paper is organized as follows. This section concludes with the notation used throughout the paper. Section II reviews norm-trace codes and their properties. Section III develops their virtual projections, allowing them to be considered as interleaved codes over a smaller field. Section IV describes how the virtual projections are used to provide a fractional decoding algorithm for these codes. The paper ends with a conclusion in Section V.

Notation. The set of nonnegative integers is denoted by $\mathbb{N}$. Given a positive integer n, $[n] := \{1, \ldots, n\}$. Given integers s and j, $\delta_{s,j} := \begin{cases} 1 & \text{if } s = j \\ 0 & \text{otherwise.} \end{cases}$ For a rational function $f \in \mathbb{F}(\mathcal{X})$ on a curve $\mathcal{X}$ and a rational point P on $\mathcal{X}$, the valuation of f at P is denoted $v_P(f)$. The multiplicative group of a field $\mathbb{F}$ is denoted by $\mathbb{F}^*$.

II. Norm-trace codes

In this section, we identify the virtual projections of the norm-trace codes which we will later use for decoding. Recall that the norm-trace curve $\mathcal{X}_{q,r}$ is defined by

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

over the finite field $\mathbb{F}_{q^r}$ with q^r elements, meaning $N(x) = Tr(y)$, where the norm $N(x) := x^u$ and the trace $Tr(y) := y^{q^{r-1}} + \ldots + y^q + y$ are taken with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ and $u = \frac{q^r-1}{q-1}$. It is well-known that the genus of $\mathcal{X}_{q,r}$ is $g = \frac{1}{2}\left(q^{r-1} - 1\right)(u-1)$.

Given $a \in \mathbb{F}_{q^r}$, consider $\Gamma_a := \{b \in \mathbb{F}_{q^r} : Tr(b) = N(a)\}$. For all $a \in \mathbb{F}_{q^r}$, $\mid \Gamma_a \mid = q^{r-1}$. The affine points of $\mathcal{X}_{q,r}$ over $\mathbb{F}_{q^r}$ are of the form $P_{ab} := (a, b)$ with $a \in \mathbb{F}_{q^r}$ and $b \in \Gamma_a$; and the set of $\mathbb{F}_{q^r}$-rational points of $\mathcal{X}_{q,r}$ is

$$\mathcal{X}_{q,r}(\mathbb{F}_{q^r}) = \{P_{ab} : a \in \mathbb{F}_{q^r}, b \in \Gamma_a\} \cup \{P_\infty\},$$

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

$$\mathcal{X}_{q,r}(\mathbb{F}_{q^r}) \setminus \{P_\infty\} = \dot{\bigcup}_{a \in \mathbb{F}_{q^r}} P_a$$

where $P_a := \{P_{ab} : b \in \Gamma_a\}$. We consider codes $C_l(\beta P_\infty) := \text{ev}\left(\mathcal{L}_l(\beta P_\infty)\right) \subseteq \mathbb{F}_{q^{rl}}^n$ in which the evaluation points

$P_1, \ldots, P_n$ are the q^{2r-1} affine points of $\mathcal{X}_{q,r}$ and the functions to evaluate are elements of

$$\mathcal{L}_l(\beta P_\infty) := \mathcal{L}(\beta P_\infty) \otimes \mathbb{F}_{q^{rl}} \subseteq \mathbb{F}_{q^{rl}}(\mathcal{X}_{q,r})$$

so that

$$\begin{array}{rccc} \text{ev}: & \mathcal{L}_l(\beta P_\infty) & \longrightarrow & \mathbb{F}_{q^{rl}}^n \\ & f & \longmapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

is injective. To guarantee that, we assume $\beta < n := q^{2r-1}$. If $2g \leq \beta < q^{2r-1}$, then $\mathcal{C}_l(\beta P_\infty)$ is an $\mathbb{F}_{q^{rl}}$-linear code over $\mathbb{F}_{q^{rl}}$, of dimension at least $\beta + 1 - g$, and with minimum distance at least $n - \beta$.

Recall that the Weierstrass semigroup of P_∞ is $H(P_\infty) = \{q^{r-1}i + uj \ : \ i, j \in \mathbb{N}\}$ which we enumerate as

$$n_1 := 0 < n_2 := q^{r-1} < n_3 < \cdots .$$

Let ρ be the monomial weight inherited from the Weierstrass semigroup so that

$$\rho(x^i y^j) := q^{r-1}i + uj.$$

Breaking ties using $x > y$, we can view ρ as a monomial order on $\mathbb{F}_{q^r}[x, y]$. Let φ_t be the maximum monomial such that $\rho(\varphi_t) = n_t$. Moreover, we define

$$\rho\left(\sum a_{ij} x^i y^j\right) := \max_{a_{ij} \neq 0} \rho(x^i y^j).$$

Observe that $\bigcup_{m \in \mathbb{N}} \mathcal{L}(mP_\infty) = \mathbb{F}_{q^r}[x, y]/(N(x) - Tr(y))$. We will identify the elements of $\mathbb{F}_{q^r}[x, y]$ with their classes in $\mathbb{F}_{q^r}[x, y]/(N(x) - Tr(y))$. Thus, monomials in $\mathbb{F}_{q^r}[x, y]$ corresponds to elements in $\mathcal{L}(mP_\infty)$ for some m where m is an upper bound on the weight ρ of the monomial. For $\beta \in \mathbb{N}$, define

$$\Phi_\beta := \left\{x^i y^j \ : \ 0 \leq i < u, \ 0 \leq j, \rho(x^i y^j) \leq \beta\right\}.$$

Then the Riemann-Roch space of a divisor βP_∞ on $\mathcal{X}_{q,r}$ satisfies

$$\mathcal{L}(\beta P_\infty) = \langle \Phi_\beta \rangle \subseteq \mathbb{F}_{q^r}[x, y].$$

III. Virtual Projections of Norm-Trace Codes

In this section, we will see how the codes $C_l(\beta P_\infty) \subseteq \mathbb{F}_{q^{rl}}^n$ can be represented over $\mathbb{F}_{q^r}$ in ways that will allow for error correction with partial information. We note that the monomial basis Φ_β is convenient, and the technique applies to other bases for $\mathcal{L}(\beta P_\infty)$, including those consisting of rational functions that are not polynomials.

Let $\{\zeta_1, \ldots, \zeta_l\}$ be a basis of $\mathbb{F}_{q^{rl}}/\mathbb{F}_{q^r}$, and let $\{\nu_1, \ldots, \nu_l\}$ be its dual basis, meaning $tr(\zeta_s \nu_j) = \delta_{s,j}$. Then for all $\beta \in F$,

$$\beta = \sum_{s=1}^{l} tr(\zeta_s \beta)\nu_s.$$

In other words, any element $\beta \in \mathbb{F}_{q^{rl}}$ can be calculated from its l projections $tr(\zeta_s \beta)$, $s \in [l]$, onto $\mathbb{F}_{q^r}$.

Definition 1. Keep the notation above and assume that $\Phi_\beta = \{h_1, \ldots, h_k\}$. For $s \in [l]$, the s-projection of the function $f(x, y) = \sum_{i=1}^k a_i h_i(x, y) \in \mathcal{L}_l(\beta P_\infty)$ to $\mathcal{L}(\beta P_\infty)$ is defined to be

$$f_s(x, y) = \sum_{i=1}^{k} tr(\zeta_s a_i) h_i(x, y).$$

Note that

$$f \in \mathcal{L}_l(\beta P_\infty) \subseteq \mathbb{F}_{q^{rl}}(\mathcal{X}) \Rightarrow f_s \in \mathcal{L}(\beta P_\infty) \subseteq \mathbb{F}_{q^r}(\mathcal{X}).$$

Furthermore, $f(x, y)$ is fully determined by $\{f_s(x, y) : s \in [l]\}$, since

$$\begin{aligned} f(x, y) &= \textstyle\sum_{i=1}^k a_i h_i(x, y) \\ &= \textstyle\sum_{i=1}^k \left[\sum_{s=1}^l tr(\zeta_s a_i)\nu_s\right] h_i(x, y) \\ &= \textstyle\sum_{s=1}^l \left[\sum_{i=1}^k tr(\zeta_s a_i) h_i(x, y)\right] \nu_s \\ &= \textstyle\sum_{s=1}^l f_s(x, y)\nu_s. \end{aligned}$$

To set the stage for fractional decoding, fix a partition

$$A_1 \dot\cup \cdots \dot\cup A_m \subseteq \{P_1, \ldots, P_n\}$$

where $m < l$. For each $t \in [m]$, consider an annihilator polynomial $p_t(x, y) \in \mathbb{F}_{q^r}[x, y]$ of a minimal degree of the set A_t, meaning

$$p_t(a, b) = 0 \ \forall (a, b) \in A_t.$$

We use this partition and the associated annihilator polynomials to define the virtual projection of functions in the Riemann-Roch space over $\mathbb{F}_{q^{rl}}$, which are inspired by the virtual projections of Reed-Solomon codes [16]–[18].

Definition 2. *Given $f \in \mathcal{L}_l(\beta P_\infty)$, $A_1 \dot\cup \cdots \dot\cup A_m \subseteq \{P_1, \ldots, P_n\}$, and $t \in [m]$, define*

$$\begin{aligned} T_t(f)(x, y) = \ & f_{l-m+t}(x, y)(p_t(x, y))^{l-m} \\ & + \textstyle\sum_{s=1}^{l-m} f_s(x, y)(p_t(x, y))^{s-1} \in \mathbb{F}_{q^r}[x, y] \end{aligned}$$

and the t-virtual projection of $\mathcal{C}_l(\beta P_\infty)$ to be

$$\mathcal{V}_t(\beta P_\infty) = \{(T_t(f)(P_1), \ldots, T_t(f)(P_n)) : f \in \mathcal{L}_l(\beta P_\infty)\}.$$

The next result demonstrates how the t-virtual projection is a subcode of a one-point norm-trace code.

Proposition 3. *The t-virtual projection $\mathcal{V}_t(\beta P_\infty)$ of $\mathcal{C}_l(\beta P_\infty)$ is a subcode of $\mathbb{F}_{q^r}^n$:*

$$\mathcal{V}_t(\beta P_\infty) \subseteq C\left((\beta - (l - m)v_{P_\infty}(p_t))\right)P_\infty.$$

Proof. Notice that

$$\mathcal{V}_t(\beta P_\infty) = \text{ev}(T_t(\mathcal{L}_l(\beta P_\infty))) \subseteq \mathbb{F}_{q^r}^n.$$

For all $f, h \in \mathcal{L}_l(\beta P_\infty)$ and $a, b \in \mathbb{F}_{q^r}$,

$$T_t \circ af + T_t \circ bh = T_t \circ (af + bh)$$

and

$$a \cdot \text{ev}\left(T_t(f)\right) + b \cdot \text{ev}\left(T_t(h)\right) = \text{ev}\left(T_t(af + bh)\right).$$

For any function $f \in \mathcal{L}_l(\beta P_\infty)$ and $t \in [m]$, $v_{P_\infty}(T_t(f))$ is bounded below by

$$\min\left\{v_{P_\infty}\left(f_i p_t^i\right), v_{P_\infty}\left(f_{l-m+t}p_t^{l-m}\right) : i \in [l-m]\right\}$$

$$\geq \min\left\{\begin{array}{ll} v_{P_\infty}(f_i) + i v_{P_\infty}(p_t), & \\ v_{P_\infty}(f_{l-m+t}) + (l-m)v_{P_\infty}(p_t) & : i \in [l-m]\end{array}\right\}$$

$$\geq \begin{cases} -\beta & \text{if } v_{P_\infty}(p_t) \geq 0 \\ -\beta + (l-m)v_{P_\infty}(p_t) & \text{if } v_{P_\infty}(p_t) < 0. \end{cases}$$

□

There are two natural sets of points to consider for a partition that gives rise to a virtual projection.

Corollary 4. 1) *Suppose $A_1' \dot\cup \cdots \dot\cup A_m' \subseteq \mathbb{F}_{q^r}$, and let $A_i = \{P_{ab} \in \mathcal{X}(\mathbb{F}_{q^r}) : a \in A_i'\}$ for $i \in [m]$. Then*

$$\mathcal{V}_t(\beta P_\infty) \subseteq C\left(\left(\beta + (l-m)|A_i'|q^{r-1}\right)P_\infty\right).$$

2) *Suppose $A_1' \dot\cup \cdots \dot\cup A_m' \subseteq \mathbb{F}_{q^r}^*$. Let D be the sum of all $\mathbb{F}_{q^r}$-rational points (a,b) of $\mathcal{X}_{q,r}$ with $a \neq 0$, and consider $A_i = \{P_{ab} \in \mathcal{X}(\mathbb{F}_{q^r}) : b \in A_i'\}$, $i \in [m]$. Then the virtual projection of the code with evaluation points in the support of D is*

$$\mathcal{V}_t(\beta P_\infty) \subseteq C\left(\left(\beta + (l-m)|A_i'|u\right)P_\infty\right).$$

We will see that a key idea to achieving fractional decoding of $C_l(\beta P_\infty)$ is decoding $\mathcal{V}_t(\beta P_\infty)$, $t \in [m]$.

Theorem 5. *Suppose $I \subseteq A_1 \dot\cup \cdots \dot\cup A_m \subseteq \{P_1, \ldots, P_n\}$, for some information set I for the code $C_l(\beta P_\infty)$. Then $f \in \mathcal{L}_l(\beta P_\infty)$ depends only on $\{T_t(f) : t \in [m]\}$ and evaluation of its elements at points in I.*

Proof. Given $A_1 \dot\cup \cdots \dot\cup A_m \subseteq \{P_1, \ldots, P_n\}$ and $\{T_t(f)(x,y) : t \in [m]\}$, we aim to determine f. For $i \in [l-m]$ and $t \in [m]$, let $T_t^{(i)}(f)(x,y) =$

$$\frac{T_t(f)(x,y) - \sum_{s=1}^{i-1} f_s(x,y)p_t(x,y)^{s-1}}{p_t(x,y)^{i-1}}.$$

First, we will determine f_1. Notice that $T_t^{(1)}(f) = T_t(f)$ and

$$f_1(P) = T_t(f)(P)$$

for all $P \in A_t$. Since $f_1 = \sum_{j=1}^k a_{1j}h_j$ for some $a_{1j} \in \mathbb{F}_{q^r}$ and $I \subseteq A_1 \cup \cdots \cup A_m$, we may use the values $h_j(P)$ for $j \in [k]$ and $P \in I$ to set up a system of equations. Since I is an information set, we can determine the a_{1j} and hence f_1.

Next, induct on $i \in [m]$, assuming that f_s, $s \in [i-1]$, is known. Notice that $T_t^{(i)}(f)$ can be determined from $T_t(f)$ and $\{f_s\}_{s=1}^{i-1}$. Since

$$T_t^{(i)}(f) = f_{l-m+t}(p_t)^{l-m-i+1} + \sum_{s=i}^{l-m} f_s(p_t)^{s-i},$$

substitution yields $f_i(P) = T_t^{(i)}(P)$ for all $P \in A_t$. Recall that $f_i = \sum_{j=1}^k a_{ij}h_j$ for some $a_{ij} \in \mathbb{F}_{q^r}$. Then using the values $h_j(P)$, $P \in I$ gives a system of k equations $f_i(P) = \sum_{j=1}^k a_{ij}h_j(P)$ in k unknowns a_{ij}, $j \in [k]$. Since I is an information set, the a_{ij} can be found, hence revealing f_i. In this way, $\{f_s(x,y) : s \in [m]\}$ may be determined, and $f(x,y) = \sum_{s=1}^l f_s(x,y)\nu_s$. □

IV. Decoding via virtual projections

In this section, we detail how virtual projections give rise to fractional decoding algorithms for norm-trace codes over extension fields.

Given a received word $w = \text{ev}(f) + e \in \mathbb{F}_{q^{rl}}^n$, for each $i \in [n]$ and $t \in [m]$, download

$$w_i^t := tr\left(\zeta_{l-m+t}w_i\right)p_t(P_i)^{l-m} + \sum_{s=1}^{l-m} tr\left(\zeta_s w_i\right)p_t(P_i)^{s-1}. \tag{1}$$

We aim to show that if e has relatively low weight, then $\text{ev}(f)$ can be recovered from

$$\pi(w) := \begin{bmatrix} w_1^1 & w_2^1 & \cdots & w_{n'}^1 \\ w_1^2 & w_2^2 & \cdots & w_{n'}^2 \\ \vdots & \vdots & & \vdots \\ w_1^m & w_2^m & \cdots & w_{n'}^m \end{bmatrix} \in \mathbb{F}_{q^r}^{m \times n'} \tag{2}$$

where $n' \leq n$ and $\{1, \ldots, n'\}$ contains an information set. Notice that if $w = \text{ev}(f)$ where $f \in \mathcal{L}_l(G)$, then

$$\begin{aligned} w_i^t &= tr\left(\zeta_{l-m+t}f(P_i)\right)p_t(P_i)^{l-m} \\ &\quad + \textstyle\sum_{s=1}^{l-m} tr\left(\zeta_s f(P_i)\right)p_t(P_i)^{s-1} \\ &= f_{l-m+t}(P_i)p_t(P_i)^{l-m} + \textstyle\sum_{s=1}^{l-m} f_s(P_i)p_t(P_i)^{s-1} \\ &= T_t(f)(P_i). \end{aligned}$$

Indeed, if $f(x,y) = \sum_{j=1}^k a_j h_j(x,y)$ where $h_j \in \mathbb{F}_{q^r}[x]$, then

$$\begin{aligned} tr\left(\zeta_s f(x,y)\right) &= tr\left(\zeta_s \sum_{j=1}^k a_j h_j(x,y)\right) \\ &= tr\left(\zeta_s \sum_{j=1}^k a_j\right) h_j(x,y). \end{aligned}$$

We have already seen in Theorem 5 that $\text{ev}(f)$ can be recovered from the array

$$\begin{bmatrix} T_1(f)(P_1) & T_1(f)(P_2) & \cdots & T_1(f)(P_{n'}) \\ T_2(f)(P_1) & T_2(f)(P_2) & \cdots & T_2(f)(P_{n'}) \\ \vdots & \vdots & & \vdots \\ T_m(f)(P_1) & T_m(f)(P_2) & \cdots & T_m(f)(P_{n'}) \end{bmatrix} \in \mathbb{F}_{q^r}^{m \times n'}.$$

The challenge now is to confirm that this is the case if $w = \text{ev}(f) + e$ where $e \in \mathbb{F}_{q^{rl}}^n$ has a positive weight, meaning some positions are in error.

We consider an approach to fractional decoding with two phases. We will write $\beta_t = \beta + (l-m)|A_i'|q^{r-1}$ or $\beta_t = \beta + (l-m)|A_i'|u$, depending on the partition in Corollary 4 used. Similar ideas apply to other partitions.

Given a received word w, download the $\pi(w)$. Then:

1) Apply a decoding algorithm for $C(\beta_t P_\infty) \subseteq \mathbb{F}_{q^r}^n$ to obtain $T_t(f)$ for all $t \in [m]$.
2) Apply Theorem 5 to obtain $\mathrm{ev}(f) \in \mathbb{F}_{q^{rl}}^n$.

In this way, the next result follows.

Theorem 6. *Suppose $I \subseteq A_1 \dot\cup \cdots \dot\cup A_m \subseteq \{P_1, \ldots, P_n\}$, for some information set I for the code $C_l(\beta P_\infty)$. The code $C_l(\beta P_\infty)$ can correct any $\left\lfloor \frac{1}{2}\left(n - \left(\beta - (l-m)\sum_{t\in[m]} v_{P_\infty}(p_t)\right) - 1\right)\right\rfloor$ errors from mn entries of $\mathbb{F}_{q^r}$.*

If $m < l$, then Theorem 6 offers an improvement in the number of symbols needed for decoding. Also, with knowledge of a subset of coordinates of size $n' < n$ containing an information set, only $mn' < ln$ symbols need to be downloaded. The performance will be dictated by the partition of the evaluation set $A_1 \dot\cup \cdots \dot\cup A_m \subseteq \{P_1, \ldots, P_n\}$ and the associated choice of annihilator functions as well as the choice of the decoding algorithm for Step (1).

Next, we consider how this approach applied is in various settings. First, recall that an error-locator is a polynomial $\Lambda \in \mathbb{F}_{q^r}[x, y]$ such that $\Lambda(P_i) = 0$ for all $i \in [n]$ with $e_i \neq 0$. The syndrome polynomial is a tool useful in finding an error-locator polynomial of minimal degree. The syndrome polynomial is defined as

$$S(x, y) = \sum_{\rho(\varphi_{i,j}) \leq \beta^\perp} s_{i,j} x^{\frac{q^r - q}{q-1} - i} y^{j_\beta - j},$$

where $s_{i,j} := \sum_{l=1}^n e_l \varphi_{i,j}(P_l)$, $j_\beta = \max\left\{j : \rho(\varphi_{i,j}) \leq \beta^\perp\right\}$, and $\beta^\perp = n + 2g - 2 - \beta$. The maximal possible order of $S(x, y)$ is $\rho_S = 2g - 1 + (j_\beta + 1)u$.

The decoding problem can be described by the following theorem, which was proven in [9] for the Hermitian case. We follow the general lines of the proof, extending the result to norm-trace codes. The Clifford defect is used to describe the number of errors correctable by the so-called key equation. Recall that the Clifford defect of a set $\mathcal{E}$ of divisors on a curve $\mathcal{X}$ is

$$s(\mathcal{E}) = \max\left\{\frac{\deg(E)}{2} - \ell(E) + 1 \ : E \in \mathcal{E}\right\}.$$

Theorem 7. *Consider a norm-trace code $C(\beta P_\infty) \subseteq \mathbb{F}_{q^r}$, received word $w = c + e$ with $c \in C(\beta P_\infty)$ and e of weight $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor - s$. Then there exists a unique polynomial $\Lambda(x, y)$ and an auxiliary polynomial $R(x, y)$ that fulfill*

$$\Lambda(x, y) S(x, y) = R(x, y) \mod y^{j_\beta + 1}, \quad (3)$$
$$\rho(R) - \rho(\Lambda) \leq \rho_S - \beta^\perp - 1 =: \ell^\star, \quad (4)$$

and $\rho(\Lambda)$ is minimal among all pairs (Λ, R) satisfying (3) and (4), where $S(x, y)$ is the syndrome polynomial associated with e. Moreover, Λ is an error-locator polynomial.

Before we prove Theorem 7, we provide an overview of how it is used for decoding $C(\beta P_\infty)$. Details are given in Algorithm 1. Given a received word $w = \mathrm{ev}(f) + e \in \mathbb{F}_{q^r}^n$ obtained from a codeword $\mathrm{ev}(f) \in C(\beta P_\infty)$, an error-locator is $\Lambda(x, y) \in \mathbb{F}_{q^r}[x, y]$ is found, along with a polynomial $R(x, y) \in \mathbb{F}_{q^r}[x, y]$ as in Equation 3. The error positions $i \in [n]$, meaning those with $e_i \neq 0$, are found by determining the roots of $\Lambda(x, y)$ among the P_i, $i \in [n]$. Then the nonzero coordinates of the error vector are given by

$$e_i = \frac{R(x, y)}{\Lambda(x, y)}.$$

Now, to prove Theorem 7, we start by proving that any error-locator is a solution to the key equation (3). To simplify the notation, we set $u_x := u$ and $u_y := q^{r-1} - 1$. We will need the following lemma, given in [10] for Hermitian codes and whose proof adapts immediately to norm-trace codes.

Lemma 8. *[10] Given an error-locator polynomial $\Lambda(x, y)$ for a received word $w = c + e$ with $c \in C(\beta P_\infty)$, meaning $e_i \neq 0 \Longrightarrow \Lambda(P_i) = 0$, there exists a polynomial $R(x, y)$ such that the pair (Λ, R) is a solution to the key equation (3).*

To guarantee that the solution in Lemma 8 is unique, we will use the following result which appears throughout the literature (see [20], for instance). We include it here (along with a short proof) for easy reference.

Proposition 9. *Let $Q = \sum_{i\in I} P_i$ for some $I \subseteq [n]$. Let ν be the smallest integer such that $\ell(\nu P_\infty - Q) \neq 0$. Let s be the Clifford defect of the curve, $\beta \geq 0$ and $d = n - \beta$. If $\mid I \mid \leq \left\lfloor \frac{d-1}{2} \right\rfloor - s$, then*

$$\ell((2g - 2 - \beta^\perp + \mu)P_\infty + Q) = 0$$

for any $\mu \leq \nu$.

Proof. Since $(2g-2)P_\infty$ is a canonical divisor, then $\mathcal{L}_\mu := \mathcal{L}((2g - 2 - \beta^\perp + \mu)P_\infty + Q)$ is isomorphic to

$$\Omega((\beta^\perp - \mu)P_\infty - Q).$$

The result for ν follows from Proposition 14 in [20]. Since $\mathcal{L}_\mu \subseteq \mathcal{L}_\nu$ for any $\mu \leq \nu$, we have the conclusion. □

We are now ready to prove Theorem 7.

Proof. Let

$$\tilde{S} = \sum_{a \leq u_x, b \leq j_\beta} s_{ab} x^{u_x - a} y^{j_\beta - b},$$

$$u_i = \frac{Tr(y) - Tr(\beta_i)}{(x - \alpha_i)(y - \beta_i)} = \frac{\mathcal{N}(x) - \mathcal{N}(\alpha_i)}{(x - \alpha_i)(y - \beta_i)},$$

and

$$U = -\sum_{i=1}^n \beta_i^{j_\beta + 1} e_i u_i$$

where $P_{\alpha_i, \beta_i} = P_i$. We have that

$$\begin{aligned}
&(y^{j_\beta+1} - \beta_i^{j_\beta+1}) \frac{\mathcal{N}(x) - \mathcal{N}(\alpha_i)}{(x - \alpha_i)(y - \beta_i)} \\
&= \sum_{k \leq u_x, h \leq j_\beta} \alpha_i^k \beta_i^h x^{u_x - k} y^{j_\beta - h} \\
&= \sum_{k \leq u_x, h \leq j_\beta} \varphi_{k,h}(P_i) x^{u_x - k} y^{j_\beta - h}.
\end{aligned}$$

Thus, $U + y^{j_\beta+1}\sum_{i=1}^{n} e_i u_i = \tilde{S}$. Let $h = \frac{\tilde{S}-U}{y^{j_\beta+1}}$.

Let (Λ, R) be a minimal solution of the key equation. Let ν be the minimal order of an error-locator polynomial. Since any error-locator polynomial is a solution, $\mu := \rho(\Lambda) \leq \nu$.

Let $\tilde{R} = R + \lambda(\tilde{S} - S)$. Observe that $\rho(\tilde{R}) \leq \rho(R)$. We have $\tilde{R} - \Lambda U = R - \Lambda S + y^{j_\beta+1}\Lambda h$. Since (Λ, R) is a solution to the key equation, we have $\tilde{R} - \Lambda U = y^{j_\beta+1}(\Lambda h + f)$ for some polynomial f. We claim that

$$\tilde{R} - \Lambda U \in \mathcal{L}((\mu + \ell^\star)P_\infty + Q - (j_\beta + 1)(u_x + 1)P_0)$$

where $Q = \sum_{\{i \,:\, e_i \neq 0\}} P_i$. Observe that $(h)_\infty \geq Q + tP_\infty$ for some integer t. Thus,

$$\tilde{R} - \Lambda U \in \mathcal{L}\left(t'P_\infty + Q - (j_\beta + 1)(u_x + 1)P_0\right).$$

We just need to compute a proper $t' \geq \rho(\tilde{R} - \Lambda U)$. We have $\rho(\tilde{R}) \leq \mu + \ell^\star$ by definition of the key equation. Observe that

$$\begin{aligned}\rho(U) &\leq \rho(Tr(y) - Tr(\beta_i)) - \rho(x - \alpha_i) - \rho(y - \beta_i)\\ &= (u_x + 1)(u_y + 1) - (u_y + 1) - (u_x + 1)\\ &= u_x u_y - 1 = 2g - 1.\end{aligned}$$

Thus, $\rho(\Lambda U) \leq \mu + 2g - 1$. Remember that

$$\ell^\star = 2g + u_x + j_\beta(u_x + 1) - \beta^\perp - 1.$$

By definition of j_β, we have that $(j_\beta+1)(u_x+1) > \beta^\perp$. Then $\ell^\star > 2g - 2$ and

$$\rho(\tilde{R} - \Lambda U) \leq \mu + \ell^\star$$

from where we have the proof of the claim.

Since $(y^{j_\beta+1}) = (j_\beta + 1)(u_x + 1)(P_0 - P_\infty)$, we have

$$\begin{aligned}&\ell((\mu + \ell^\star)P_\infty + Q - (j_\beta + 1)(u_x + 1)P_0)\\ =&\ell((\mu + \ell^\star - (j_\beta + 1)(u_x + 1))P_\infty + Q).\end{aligned}$$

Given $\mu+\ell^\star-(j_\beta+1)(u_x+1) = \mu+2g-2-\beta^\perp$ and $\mu \leq \nu$, by Proposition 9, we have that $\tilde{R} - \Lambda U = 0$, which is $\tilde{R} = \Lambda U$. Since $\tilde{R}$ is a polynomial, then $(\Lambda)_0 \geq (U)_\infty - \rho(U)P_\infty = Q$ and we obtain that Λ is an error-locator polynomial of minimal degree. □

The main part of the division decoding algorithm proposed by Kampf in [9] based on the polynomial division, proposed a division decoding algorithm to locate all error patterns of weight up to $\left\lfloor \frac{d-1}{2} \right\rfloor - s$. The basic idea is the construction of two sequences of polynomials $\Delta_i(x, y)$ and $R_i(x, y)$, each pair fulfilling

$$\Delta_i(x, y)S(x, y) = R_i(x, y) \mod y^{j_\beta+1} \tag{5}$$

where $\rho(\Delta_i) = \rho(\varphi_i)$ and $\rho(R_i)$ is minimal, given $\rho(\Delta_i)$; that is, the method consists in obtain a candidate error-locator of each possible order, so as soon as $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor - s$ we can find a pair (Δ_i, R_i) that fulfills

$$\rho(R_i) - \rho(\Delta_i) \leq \ell^\star, \tag{6}$$

then we set $\Lambda(x, y) = \Delta_i(x, y)$ and $R(x, y) = R_i(x, y)$, which is the wanted solution to the key equation (3). A pseudocode for this method is given in Algorithm 1.

Algorithm 1 Solving the key equation for norm-trace codes

Input: Polynomial $S \neq 0$, $y^{j_\beta+1}$; constant $\ell^\star$.
Output: Locator polynomial Λ, evaluator polynomial R.
Initialization: $i = 0, \Delta_0 = 1, R_0 = S$
repeat
$i = i + 1$
if $\varphi_i = x^a$ then $\varphi_{i_1} = x^{a-1}$, else $\varphi_{i_1} = \frac{\varphi_i}{y}$
$\theta = \frac{\varphi_i}{\varphi_{i_1}} R_{i_1} \mod (N(x) - Tr(y),\ y^{j_\beta+1})$.
Divide θ by $R_{i-1}, \ldots, R_0 : \theta = \sum_j \gamma_{i,j} R_j + R_i$
$\gamma_{i,i_1} = \gamma_{i,i_1} - \frac{\varphi_i}{\varphi_{i_1}}$
$\Delta_i = -\sum_j \gamma_{i,j}\Delta_j$
until $\rho(R_i) - \rho(\Delta_i) \leq \ell^\star$
$\Lambda = \Delta_i, R = R_i$.

Since we are only interested in the zeros of the locator polynomial, Algorithm 1 always considers monic polynomials. The polynomial $\Delta_i(x, y)$ will therefore be of the form $\Delta_i(x, y) = \varphi_i(x, y) + \sum_{j=0}^{i-1} \alpha_j \varphi_j(x, y)$ with constants $\alpha_j \in \mathbb{F}_{q^r}$.

To complete the decoding process, it is necessary to determine the error positions and values so that the codeword can be recovered. The error values are given by the residues of $R(x, y)/\Lambda(x, y)$, meaning the error word (and hence codeword) can be recovered from the output of Algorithm 1. In particular,

$$c = w - \sum_{i \in [n] \Lambda(x_i, y_i) = 0} \frac{R(x_i, y_i)}{\Lambda(x_i, y_i)}$$

provided $wt(e) \leq \left\lfloor \frac{n-\beta}{2} - s \right\rfloor$.

Finally, we give a fractional decoding of the constant extension norm-trace codes as in Algorithm 2, and we utilize the key equation for norm-trace codes.

Algorithm 2 Fractional decoding of constant extension norm-trace codes

Input: Received word $w = \text{ev}(f) + e$ where $f \in \mathcal{L}_l(\beta P_\infty)$ and $I \subseteq A_1 \dot\cup \ldots \dot\cup A_m \subseteq \{P_1, \ldots, P_n\}$ for some information set I of $C_l(\beta P_\infty)$.
Output: $\text{ev}(f) \in \mathcal{C}_l(\beta P_\infty)$, provided $wt(e) \leq \left\lfloor \frac{n-\beta}{2} - s \right\rfloor$
for $t = 1, \ldots, m$
Download d_i^t, $i \in [n]$, as in Equation 1.
Apply Algorithm in 1 to recover $T_t(f)$.
Apply Theorem 5 to recover $\text{ev}(f)$.

V. Conclusion

In this paper, we provide a fractional decoding algorithm for codes from the norm-trace curve, allowing one to perform decoding using a fraction $\frac{m}{l} < 1$ of symbols of the base field to represent a received word. While the error-correcting capability is less than that of the original code, fewer symbols are needed for recovering the original codeword. Furthermore, these codes allow for longer constructions than those with error correction from partial information in the literature.

REFERENCES

[1] A. Brown, L. Minder, A. Shokrollahi, *Improved Decoding of Interleaved AG Codes*, Lecture Notes in Computer Science, vol. 3796, pp. 37-46,2005.

[2] 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, vol. 56, no. 9, pp. 4539-4551, 2010.

[3] 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, vol. 67, no. 10, pp. 6619-6626, 2021.

[4] S. Ghemawat, H. Gobioff, and S. Leung, *The Google File System*, Proceedings of 19th ACM Symposium on Operating Systems Principles, pp. 29-43, 2003.

[5] V. Guruswami and M. Wootters, Repairing Reed-Solomon Codes, IEEE Transactions on Information Theory, vol. 63, no. 9, pp. 5684-5698, 2017.

[6] V. Guruswami and C. Xing, *List Decoding Reed-Solomon, Algebraic-Geometric, and Gabidulin Subcodes up to the Singleton Bound*, Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing (STOC '13). Association for Computing Machinery, pp. 843–852, 2013.

[7] T. Høholdt and R. R. Nielsen, *Decoding Hermitian Codes with Sudan's Algorithm*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science, vol 1719, 1999.

[8] C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, and S. Yekhanin, *Erasure Coding in Windows Azure Storage*, USENIX Annual Technical Conference, pp. 15-26, 2012.

[9] S. Kampf, M. Bossert, and I. Bouw, *Solving the Key Equation for Hermitian Codes with a Division Algorithm*, IEEE International Symposium on Information Theory (ISIT), pp. 1008-1012, 2011.

[10] S. Kampf, *Bounds on Collaborative Decoding of Interleaved Hermitian Codes and Virtual Extension*. Designs, Codes and Cryptography, vol. 70, pp. 9–25, 2014.

[11] 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*, Proceedings of 9th International Conference on Architectural Support for Programming Languages and Operating Systems, pp. 190-201, 2000.

[12] H. H. López and G. L. Matthews, *Multivariate Goppa Codes*, IEEE Transactions on Information Theory, vol. 69, no. 1, pp. 126-137, 2023.

[13] G. L. Matthews, A. W. Murphy, and W. Santos, *Fractional Decoding of Codes from Hermitian curves*, IEEE International Symposium on Information Theory (ISIT), pp. 515-520, 2021.

[14] G. L. Matthews, A. W. Murphy, and W. Santos, *Fractional decoding r-Hermitian codes*, Finite Fields and Their Applications, vol. 92, 2023.

[15] W. Santos, *On Fractional Decoding of Reed-Solomon Codes*, IEEE International Symposium on Information Theory (ISIT), pp. 1552-1556, 2019.

[16] I. Tamo, M. Ye, and A. Barg, *Fractional Decoding: Error Correction from Partial Information*, 2017 IEEE International Symposium on Information Theory (ISIT), pp. 998-1002, 2017.

[17] I. Tamo, M. Ye and A. Barg, "Error Correction Based on Partial Information, IEEE Transactions on Information Theory, vol. 66, no. 3, pp. 1396-1404, 2020.

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

[19] Stichtenoth H., *Algebraic Functions Fields and Codes*, Springer, Berlin, 1993.

[20] S. C. Porter, B-Z. Shen, and R. Pellikaan. *Decoding geometric Goppa codes using an extra place*, IEEE Transactions on Information Theory, vol. 38, no. 6, pp. 1663-1676, 1999.

[21] S. Puchinger, J. Rosenkilde, and I. Bouw, Improved power decoding of interleaved one-point Hermitian codes, Designs, Codes and Cryptography, vol. 87, pp. 589–607, 2019.

[22] M. Ye and A. Barg, Explicit constructions of MDS array codes and RS codes with optimal repair bandwidth, 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, Spain, 2016, pp. 1202-1206.