there is a one-to-one correspondence between the elements of $\mathcal{B}$ and the rows of $T$.

By performing row operations on $T$, we can obtain a vector $\boldsymbol{c} \in C$ whose projection onto the coordinates corresponding to the places lying over $P_\alpha$ equals $(1, 0, \ldots, 0)$, where the first coordinate corresponds to $P_1$ (the number of operations in this stage is of the order of $n^3$). As a result, we also obtain an element $z \in \mathcal{L}(m'Q)$ such that $\boldsymbol{c} = \phi_G(z)$, where $G := m'Q$. Note that $v_{P_1}(z) = 0$, and $v_P(z) \geq 1$ for all the other places of $F$ lying over $P_\alpha$. Now we claim that we may define $e_1 := z/(x_0 - \alpha)$.

*Proposition 4.10:* Maintaining the above notation, we have

$$\frac{z}{x_0 - \alpha} \in \mathcal{L}((2g-1)Q + P_1) \backslash \mathcal{L}((2g-1)Q).$$

*Proof:* We have

$$\begin{aligned}\left(\frac{1}{x_0 - \alpha}\right) &= \mathrm{Con}_{F/\mathbb{F}_q(x_0)}(P_\infty - P_\alpha) \\ &= \sqrt{q}^s Q - \mathrm{Con}_{F/\mathbb{F}_q(x_0)}(P_\alpha)\end{aligned}$$

where $\mathrm{Con}_{F/\mathbb{F}_q(x_0)}$ stands for the *conorm map*. Let $e_1 := z/(x_0 - \alpha)$. Since $v_Q(z) \geq -(2g - 1 + \sqrt{q}^s)$, we have $v_Q(e_1) \geq -(2g-1)$. In addition, $v_{P_1}(e_1) = -1$, and $v_P(e_1) \geq 0$ for all places of $F$ not in $\{Q, P_1\}$. □

In practice, we can use the method described above to construct simultaneously all the elements $e_i$ corresponding to the places lying over some place $P_\alpha$ of $\mathbb{F}_q(x_0)$, where $\alpha \in \Omega^c$. This can be done by Gaussian elimination, which requires $O(n^3)$ $\mathbb{F}_q$ operations. Hence, after the generator matrix $T$ is constructed in $\leq (n \log_{\sqrt{q}} n)^3$ operations, all the elements $e_i$, $i \in \{1, 2, \ldots, n\}$, can be found by $< q$ runs of an algorithm of complexity of the order of $n^3$.

## ACKNOWLEDGMENT

The author is grateful to Prof. C. P. Xing for kindly letting him have a copy of [8] and for allowing him to include the material of Section III-A in the manuscript. The author would also like to thank the anonymous referees for their valuable comments, and especially one of the referees for pointing out that the elements $\{e_i\}$ can be constructed in polynomial time.

## REFERENCES

[1] A. Garcia and H. Stichtenoth, "On the asymptotic behavior of some towers of function fields over finite fields," *J. Number Theory*, vol. 61, pp. 248–273, 1996.

[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[3] K. W. Shum, I. Aleshnikov, P. V. Kumar, H. Stichtenoth, and V. Deolalikar, "A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert–Varshamov bound," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2225–2241, Sept. 2001.

[4] H. Stichtenoth, *Algebraic Function Fields and Codes*. Berlin, Germany: Springer-Verlag, 1993.

[5] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-Geometric Codes*. Dordrecht, The Netherlands: Kluwer, 1991.

[6] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, "Modular codes, Shimura curves, and Goppa codes, better than the Varshamov–Gilbert bound," *Math. Nachrichtentech.*, vol. 109, pp. 21–28, 1982.

[7] C. P. Xing, "Nonlinear codes from algebraic curves improving the Tsfasman–Vlăduţ–Zink bound," *IEEE Trans. Inform. Theory*, vol. 49, pp. 1653–1657, July 2003.

[8] ——, "An explicit construction of nonlinear codes," unpublished manuscript, 2004.

# On the Structure of Hermitian Codes and Decoding for Burst Errors

Jian Ren, *Member, IEEE*

***Abstract*—In this correspondence, it is proved that Hermitian code is a direct sum of concatenated Reed–Solomon codes over GF $(q^2)$. Based on this discovery, first, a new method for computing the dimension and tightly estimating the minimum distance of the Hermitian code is derived. Secondly, a new decoding algorithm, which is especially effective in dealing with burst errors with complexity $O(n^{5/3})$, is described. Finally, some possible approaches for optimization of Hermitian codes are discussed.**

***Index Terms*—Burst error, concatenation, decoding algorithm, Hermitian code, Reed–Solomon code.**

## I. INTRODUCTION

One of the most important development in the theory of error-correcting codes in recent years has been the introduction of methods from algebraic curves to construct good linear codes. Since then, much attention from mathematicians and coding theorists alike has been focused on the study of algebraic-geometry codes and some excellent works have emerged [1]–[5], many of which are concerned with the decoding of random errors. In fact, algebraic-geometry codes can also be used to correct burst errors very effectively and efficiently.

This correspondence studies the structure of Hermitian codes [6]–[9] and decoding of Hermitian codes for burst errors. First, a new method for computing the dimension and tightly estimating the minimal distance of the Hermitian code is derived. Secondly, a new decoding algorithm is presented. This decoding algorithm is especially effective in dealing with burst errors with complexity only $O(n^{5/3})$. Some possible approaches for Hermitian codes optimization are also briefly mentioned.

This correspondence is organized as follows: In Section II, several frequently used results in the theory of Hermitian codes are presented. The structure of Hermitian codes and their parameters are studied in Section III. In Section IV, a decoding algorithm that is especially efficient in correcting burst errors for Hermitian codes is given. An illustrative decoding example is presented in Section V. In Section VI, several possible approaches for optimization of Hermitian codes are pointed out. Finally, we conclude in Section VII with some further discussions and suggestions.

## II. BASIC THEORY OF HERMITIAN CODES

A Hermitian curve $\mathcal{H}(q)$ (see [7]–[9]) over GF$(q^2)$ in affine coordinates is defined by

$$\mathcal{H}(q) : y^q + y = x^{q+1}. \tag{1}$$

The genus of $\mathcal{H}(q)$ is $g = (q^2 - q)/2$ and there are $q^3 + 1$ rational points on $\mathcal{H}(q)$, of which there are $n = q^3$ points that satisfy (1), denoted as $R_0, R_1, \ldots, R_{n-1}$, and $Q$, the point at infinity.

The following proposition from [7], [9] plays an important role in this correspondence, we present it here without proof.

Manuscript received November 20, 2003; revised July 9, 2004.

The author is with the Department of Electrical and Computer Engineering, Michigan State University, East Landing, MI 48864-1226 USA (e-mail: renjian@egr.msu.edu).

Communicated by G. Zémor, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2004.836918

*Proposition 1:* For each $m \geq 0$, the following set is a basis of $L(mQ)$:

$$\left\{x^t y^j \mid 0 \leq t, 0 \leq j \leq q-1, tq + j(q+1) \leq m\right\}.$$

Hermitian code is defined as $\mathcal{H}_m = C(D, mQ)$, where $D = R_0 + R_1 + \cdots + R_{n-1}$ with $n = q^3$.

From [9] we know that $y^q + y = 0$ has $q$ solutions in GF$(q^2)$. Let $\mathcal{B} = \{\beta_0, \beta_1, \ldots, \beta_{q-1}\}$ be the $q$ solutions. Assume that $(1, y_0)$ is a solution to (1), then according to [9], the $q^3$ rational points on Hermitian curve $\mathcal{H}(q)$ can be represented as $(\eta, \eta^{q+1} y_0 + \beta_j)$, where $\eta \in$ GF$(q^2)$, $j = 0, 1, \ldots, q-1$.

Suppose $\alpha$ is a primitive element in GF$(q^2)$, let $y_0 = \alpha$, then the $q^3$ rational points on Hermitian curve can be expressed as

$$(\alpha^{s_i}, \alpha^{s_i(q+1)+1} + \beta_j)$$

where $i = 0, 1, \ldots, q^2 - 1$, $j = 0, 1, \ldots, q-1$, $s_i = i - 1$ if $i \geq 1$, while $s_0 = -\infty$, and $\alpha^{-\infty} = 0$.

Thus, the $q^3$ rational points can be represented as the first expression at the bottom of the page.

Define the following parameters associated with Hermitian code $\mathcal{H}_m$ over GF$(q^2)$

$$k(j) = \max\{t \mid tq + j(q+1) \leq m\} + 1 \tag{2}$$

$$\tau = \min\left\{q-1, \left\lfloor \frac{m}{q+1} \right\rfloor\right\}. \tag{3}$$

Then we have the following proposition.

*Proposition 2:* See the second equation at the bottom of the page. Therefore, an element of $\mathcal{H}_m$ is of the form

$$(g(R_0), g(R_1), \ldots, g(R_{q^3-1}))$$

where

$$g(x, y) = f_0(x) + y f_1(x) + \cdots + y^\tau f_\tau(x)$$

with $\deg f_{j_\tau}(x) < k(j_\tau)$ for $j_\tau = 0, 1, \ldots, \tau$ and $g(R_v)$ means to substitute $x$ and $y$ in $g(x, y)$ with the first and the second coordinates of $R_v$, respectively, $v = 0, 1, \ldots, n-1$.

In particular, if $m \geq q^2 - 1$, then $\tau = q - 1$. From this point on, our discussion will be limited to $m \geq q^2 - 1$.

## III. The Structure of Hermitian Codes

Let $\mathcal{G}_j$ be as in the third equation at the bottom of the page. Then we have the following theorem.

*Theorem 1:* Let $\mathcal{H}_m$ and $\mathcal{G}_j$ $(j = 0, 1, \ldots, q-1)$ be the linear codes defined as in the third equation at the bottom of the page, then

$$\mathcal{H}_m = \mathcal{G}_0 \oplus \mathcal{G}_1 \oplus \mathcal{G}_2 \oplus \cdots \oplus \mathcal{G}_{q-1}$$

where $\oplus$ denotes direct sum of vector spaces.

*Proof:* $\mathcal{H}_m = \mathcal{G}_0 + \mathcal{G}_1 + \mathcal{G}_2 + \cdots + \mathcal{G}_{q-1}$ follows directly from Proposition 2. The proof that the sum is direct follows from Section IV. □

Since only one element in $\mathcal{B}$ is zero, we may assume that $\beta_0 = 0$, then $\beta_1, \beta_2, \ldots, \beta_{q-1}$ are all nonzero elements in GF$(q^2)$. Correspondingly, of all the rational points, only $R_0$ has the second coordinate equal to zero, that is, $y(R_0) = 0$. Therefore, $\mathcal{G}_j$ is defined as in the fourth equation at the bottom of the page, where $c = 1$ if $f_0 = 1$, and $c = 0$ otherwise.

*Definition 1:* The extended Reed–Solomon code ERS$_q(k, q)$ and the Reed–Solomon code RS$_q(k, q)$ over GF$(q)$ are defined as in the fifth expression at the bottom of the page [10], where GF$(q) = \{0, 1, \alpha, \ldots, \alpha^{q-2}\}$.

It is clear that ERS$_q(k, q)$ is a $[q, k, q-k+1]_q$ code and RS$_q(k, q)$ is a $[q-1, k, q-k]_q$ code.

---

$$\begin{array}{llll} R_0 = (0, \beta_0) & R_1 = (1, \alpha + \beta_0) & \cdots & R_{q^2-1} = (\alpha^{q^2-2}, \alpha^{(q^2-2)(q+1)+1} + \beta_0) \\ R_{q^2} = (0, \beta_1) & R_{q^2+1} = (1, \alpha + \beta_1) & \cdots & R_{2q^2-1} = (\alpha^{q^2-2}, \alpha^{(q^2-2)(q+1)+1} + \beta_1) \\ \vdots & \vdots & \ddots & \vdots \\ R_{q^2(q-1)} = (0, \beta_{q-1}) & R_{q^2(q-1)+1} = (1, \alpha + \beta_{q-1}) & \cdots & R_{q^3-1} = (\alpha^{q^2-2}, \alpha^{(q^2-2)(q+1)+1} + \beta_{q-1}). \end{array}$$

---

$$L(mQ) = \left\{f_0(x) + y f_1(x) + \cdots + y^\tau f_\tau(x) \mid \deg f_{j_\tau}(x) < k(j_\tau), j_\tau = 0, 1, \ldots, \tau\right\}.$$

---

$$\mathcal{G}_j = \left\{\left((y^j f_j)(R_0), (y^j f_j)(R_1), \ldots, (y^j f_j)(R_{q^3-1})\right) \mid \deg f_j < k(j)\right\},\ j = 0, 1, \ldots, q-1.$$

---

$$\mathcal{G}_j = \left\{\left(c, (y^j f_j)(R_1), (y^j f_j)(R_2), \ldots, (y^j f_j)(R_{q^3-1})\right) \mid \deg f_j < k(j)\right\}, j = 0, 1, \ldots, q-1$$

---

$$\text{ERS}_q(k, q) = \left\{(f(0), f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \mid f(x) \in \text{GF}(q)[x] \text{ and } \deg f(x) < k\right\}$$

$$\text{RS}_q(k, q) = \left\{(f(1), f(\alpha), \ldots, f(\alpha^{q-2})) \mid f(x) \in \text{GF}(q)[x] \text{ and } \deg f(x) < k\right\}$$

Let us define $\boldsymbol{G}_{j,l}$ as in the first equation at the bottom of the page. Then it is easy to show the following proposition.

*Proposition 3:*

$\boldsymbol{G}_{j,l} \cong \mathrm{ERS}_{q^2}(k(j), q^2), j = 0, 1, \ldots, q-1, l = 1, \ldots, q-1.$

$\boldsymbol{G}_{j,0} \cong RS_{q^2}(k(j), q^2), j = 0, 1, \ldots, q-1.$

Suppose $C$ and $D$ are two linear codes, the concatenation of code $C$, and code $D$ is denoted as $C\|D$, which is defined in the second equation at the bottom of the page.

From Theorem 1 and Proposition 3, we immediately have the following theorem.

*Theorem 2:* For $j = 0, \ldots, q-1$,

$$\mathcal{G}_j = \left(\boldsymbol{G}_{j,0}\|\boldsymbol{G}_{j,1}\|\boldsymbol{G}_{j,2}\|\cdots\|\boldsymbol{G}_{j,q-1}\right)$$
$$\cong \Big(\mathrm{RS}_{q^2}(k(j), q^2)\| \underbrace{\mathrm{ERS}_{q^2}(k(j), q^2)\|\cdots\|\mathrm{ERS}_{q^2}(k(j), q^2)}_{q-1 \text{ times}}\Big).$$

$$\mathcal{H}_m = \left(\boldsymbol{G}_{0,0}\|\boldsymbol{G}_{0,1}\|\cdots\|\boldsymbol{G}_{0,q-1}\right) \oplus \left(\boldsymbol{G}_{1,0}\|\boldsymbol{G}_{1,1}\|\cdots\|\boldsymbol{G}_{1,q-1}\right) \oplus \cdots \oplus \left(\boldsymbol{G}_{q-1,0}\|\boldsymbol{G}_{q-1,1}\|\cdots\|\boldsymbol{G}_{q-1,q-1}\right).$$

Since $\boldsymbol{G}_{0,0}$ is a generalized Reed–Solomon code with parameters $[q^2, k(0), q^2 - k(0)]$. $\boldsymbol{G}_{j,0}$ is a Reed–Solomon code with parameters $[q^2, k(j), q^2 + 1 - k(j)]$ for $j = 1, 2, \ldots, q-1$. Therefore, $\mathcal{G}_0$ is a $[q^3, k(0), q^3 + q - qk(0)]$ code and $\mathcal{G}_j$ is a $[q^3, k(j), q^3 + q - 1 - qk(j)]$ code for $j = 1, 2, \ldots, q-1$.

*Corollary 1:* The Hermitian code over $\mathrm{GF}(q^2)$ is a direct sum of concatenated Reed–Solomon codes. Moreover

$$\dim(\mathcal{H}_m) = k(0) + k(1) + k(2) + \cdots + k(q-1)$$
$$\mathrm{dist}(\mathcal{H}_m) \le \min_{0 \le j \le q-1}\{q^3 + q - qk(j)\} = q^3 - q\left\lfloor \frac{m}{q} \right\rfloor$$

where $\dim$ stands for dimension and $\mathrm{dist}$ stands for minimum distance.

In particular, for $m = 0 \pmod q$, we have $\mathrm{dist}(\mathcal{H}_m) \le q^3 - m$. This upper bound is the true minimum distance according to [6]. Even for $m \neq 0 \pmod q$, although the upper bound for the minimum distance may not always be the true minimum distance, it can be very tight. For example, when $q = 4, m = 37$, we have

$$\mathrm{dist}(\mathcal{H}_m) = \mathrm{dist}(\mathcal{H}_{37}) \le q^3 - q\lfloor m/q \rfloor = 28.$$

On the other hand, by [8] we know $\mathrm{dist}(\mathcal{H}_m) \ge 27$, therefore, $27 \le \mathrm{dist}(\mathcal{H}_m) \le 28$.

*Remark 1:* The actual minimum distance for Hermitian codes is known [6].

*Remark 2:* Corollary 1 was partly obtained in [9], however, our method is much easier to understand.

## IV. Decoding Algorithm

In this section, a new decoding algorithm for Hermitian code with emphasis on burst errors is described.

Arrange the $q^3$ rational points in the following table: the third expression at the bottom of the page. That is,

$$P_{i,l} \triangleq R_{lq^2+i}, \qquad i = 0, 1, \ldots, q^2 - 1, l = 0, 1, \ldots, q-1.$$

Noting that for each $i = 0, 1, \ldots, q^2 - 1$, the rational points $P_{i,0}, P_{i,1}, \ldots, P_{i,q-1}$ all have the same first coordinate. Rewrite the Hermitian code $\mathcal{H}_m$ as the fourth expression at the bottom of the page.

Let

$$\boldsymbol{r} = \Big(g(P_{0,0}), \ldots, g(P_{0,q-1}), \ldots, g(P_{q^2-1,0}), \ldots, g(P_{q^2-1,q-1})\Big)$$

be a transmitted codeword, where $g \in L(mQ)$ and

$$\boldsymbol{u} = (u_{0,0}, \ldots, u_{0,q-1}, \ldots, u_{q^2-1,0}, \ldots, u_{q^2-1,q-1})$$

be the received code.

Since $g \in L(mQ)$, we may assume

$$g(P_{i,l}) = f_0(P_{i,l}) + y(P_{i,l})f_1(P_{i,l}) + \cdots + y^{q-1}(P_{i,l})f_{q-1}(P_{i,l}), \quad i = 0, 1, \ldots, q^2 - 1, l = 0, 1, \ldots, q-1$$

where

$$\deg f_j(x) < k(j), \qquad \text{for } j = 0, 1, \ldots, q-1.$$

Since $P_{i,0}, P_{i,1}, \ldots, P_{i,q-1}$ all have the same first coordinate, and $f_j(P_{i,l})$ is only applied to the first coordinate of $P_{i,l}$, therefore, $f_j(P_{i,l})$ does not depend on $l$. In fact, $f_j(P_{i,l}) = f_j(\alpha^{s_i})$, where $i = 0, 1, \ldots, q^2 - 1$ and $s_i = i - 1$ if $i \ge 1$, while $s_0 = -\infty$, and $\alpha^{-\infty} = 0$.

Substitute $f_j(P_{i,l})$ and $g(P_{i,l})$ with $x_{ji}$ and $u_{il}$, respectively, and treat $x_{ji}$ as an indeterminate. From the $q$ rational points in group $i$, that is, $P_{i,0}, P_{i,1}, \ldots, P_{i,q-1}$, we derive the following $q^2$ different set of equations ($i = 0, 1, \ldots, q^2 - 1$):

$$\begin{cases} x_{0,i} + y(P_{i,0})x_{1,i} + \cdots + (y(P_{i,0}))^{q-1}x_{q-1,i} = u_{i,0} \\ x_{0,i} + y(P_{i,1})x_{1,i} + \cdots + (y(P_{i,1}))^{q-1}x_{q-1,i} = u_{i,1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_{0,i} + y(P_{i,q-1})x_{1,i} + \cdots + (y(P_{i,q-1}))^{q-1}x_{q-1,i} = u_{i,q-1} \end{cases}. \quad (4)$$

---

$$\boldsymbol{G}_{j,l} = \left\{\Big((y^j f_j)(R_{lq^2}), (y^j f_j)(R_{lq^2+1}), \ldots, (y^j f_j)(R_{lq^2+q^2-1})\Big) \mid \deg f_j < k(j)\right\}, \qquad j = 0, 1, \ldots, q-1, l = 0, 1, \ldots, q-1.$$

---

$$C\|D = \left\{(c_1, c_2, \ldots, c_r, d_1, d_2, \ldots, d_s) \mid (c_1, c_2, \ldots, c_r) \in C,\ (d_1, d_2, \ldots, d_s) \in D\right\}.$$

---

$$\begin{array}{cccc} P_{0,0} = (0, \beta_0) & P_{1,0} = (1, \alpha + \beta_0) & \cdots & P_{q^2-1,0} = (\alpha^{q^2-2}, \alpha^{(q^2-2)(q+1)+1} + \beta_0) \\ P_{0,1} = (0, \beta_1) & P_{1,1} = (1, \alpha + \beta_1) & \cdots & P_{q^2-1,1} = (\alpha^{q^2-2}, \alpha^{(q^2-2)(q+1)+1} + \beta_1) \\ \vdots & \vdots & \ddots & \vdots \\ P_{0,q-1} = (0, \beta_{q-1}) & P_{1,q-1} = (1, \alpha + \beta_{q-1}) & \cdots & P_{q^2-1,q-1} = (\alpha^{q^2-2}, \alpha^{(q^2-2)(q+1)+1} + \beta_{q-1}) \end{array}.$$

---

$$\mathcal{H}_m = \left\{\Big(g(P_{0,0}), \ldots, g(P_{0,q-1}), \ldots, g(P_{q^2-1,0}), \ldots, g(P_{q^2-1,q-1})\Big) \mid g \in L(mQ)\right\}.$$

Because the coefficient matrix for the system of equations (4) is a Vandermonde matrix, it has a unique solution. Clearly, when

$$\boldsymbol{u} = (u_{0,0}, \ldots, u_{0,q-1}, \ldots, u_{q^2-1,0}, \ldots, u_{q^2-1,q-1})$$

is a codeword, then by solving $(x_{0,i}, x_{1,i}, \ldots, x_{q-1,i})$ from the system of equations (4), $i = 0, 1, \ldots, q^2 - 1$, we get $q^2$ solutions

$$\Big(f_0(\alpha^{s_i}), f_1(\alpha^{s_i}), \ldots, f_{q-1}(\alpha^{s_i})\Big), \qquad i = 0, 1, \ldots, q^2 - 1.$$

Let

$$\boldsymbol{r}_j = \Big(f_j(0), f_j(1), f_j(\alpha), \ldots, f_j(\alpha^{q^2-2})\Big), \qquad j = 0, 1, \ldots, q-1. \tag{5}$$

Then $\boldsymbol{r}_j$ is an extended Reed–Solomon codeword [10], [11]. Whenever $\boldsymbol{u} = (u_{0,0}, \ldots, u_{0,q-1}, \ldots, u_{q^2-1,0}, \ldots, u_{q^2-1,q-1})$ has errors, then there exists at least one $j$ such that $\boldsymbol{r}_j$ is with errors. Therefore, we can decode ([10], [11]) $\boldsymbol{r}_j$ as an extended Reed–Solomon code to recover the error vector $\boldsymbol{e}_j$, $j = q-1, q-2, \ldots, 1, 0$.

Now, let us formulate the decoding procedures in the follows algorithm, which is in fact more efficient.

**Decoding Algorithm:**

Step 1: Substitute the transmitted codeword

$$\boldsymbol{c} = \Big(g(P_{0,0}), \ldots, g(P_{0,q-1}), \ldots, g(P_{q^2-1,0}), \ldots, g(P_{q^2-1,q-1})\Big)$$

with the received word $\boldsymbol{u} = (u_0, u_1, \ldots, u_{q^3-1})$ in the system of equations (4). Construct $\boldsymbol{r}_j$ given in (5) by solving the (4), $j = 0, 1, \ldots, q-1$. If $\boldsymbol{u}$ has transmission error(s), then at least one $\boldsymbol{r}_j$ will have error(s).

Step 2: Decode $\boldsymbol{r}_{q-1}$ in $\mathrm{ERS}_{q^2}(k(q-1), q^2)$ using the decoding algorithm of extended Reed–Solomon code (see for example [10], [11]). Suppose the error vector is

$$\boldsymbol{e}_{q-1} = (e_{q-1,0}, e_{q-1,1}, \ldots, e_{q-1,q^2-1})$$

and the error locations are $E_{q-1,1}, E_{q-1,2}, \ldots, E_{q-1,t_1}$. Then $\boldsymbol{r}_{q-1} - \boldsymbol{e}_{q-1}$ is a codeword in $\mathrm{ERS}_{q^2}(k(q-1), q^2)$. Substitute $\boldsymbol{r}_{q-1}$ with $\boldsymbol{r}_{q-1} - \boldsymbol{e}_{q-1}$.

Step 3: Mark the locations of $E_{q-1,1}, E_{q-1,2}, \ldots, E_{q-1,t_1}$ in $\boldsymbol{r}_{q-2}$ with "$\otimes$" and treat these locations as erasures. Decode $\boldsymbol{r}_{q-2}$ in $\mathrm{ERS}_{q^2}(k(q-2), q^2)$ using the decoding algorithm of extended Reed–Solomon code. Suppose the error vector is

$$\boldsymbol{e}_{q-2} = (e_{q-2,0}, e_{q-2,1}, \ldots, e_{q-2,q^2-1})$$

and the new error locations are $E_{q-2,1}, E_{q-2,2}, \ldots, E_{q-2,t_2}$. Now $\boldsymbol{r}_{q-2} - \boldsymbol{e}_{q-2}$ is a codeword in $\mathrm{ERS}_{q^2}(k(q-2), q^2)$. Substitute $\boldsymbol{r}_{q-2}$ with $\boldsymbol{r}_{q-2} - \boldsymbol{e}_{q-2}$.

Step 4: Repeat Step 3 for $\boldsymbol{r}_j$ and let $\boldsymbol{e}_j$ be the error vector, $j = q-3, q-4, \ldots, 1, 0$.

Step 5: Substitute $(x_{0,i}, x_{1,i}, \ldots, x_{q-1,i})$ in the system of equations (4) with $(e_{0,i}, e_{1,i}, \ldots, e_{q-1,i})$, and then compute the left-hand side, we get

$$(\overline{e}_{0,i}, \overline{e}_{1,i}, \ldots, \overline{e}_{q-1,i}), \qquad i = 0, 1, \ldots, q^2 - 1.$$

Finally, we get the error vector

$$\boldsymbol{e} = (\overline{e}_{0,0}, \ldots, \overline{e}_{0,q-1}, \ldots, \overline{e}_{q^2-1,0}, \ldots, \overline{e}_{q^2-1,q-1})$$

for the received codeword

$$\boldsymbol{u} = (u_{0,0}, \ldots, u_{0,q-1}, \ldots, u_{q^2-1,0}, \ldots, u_{q^2-1,q-1})$$

Hence, the transmitted codeword is $\boldsymbol{u} - \boldsymbol{e}$ and the decoding is done.

Let $C(j)$ denote the decoding complexity for the $j$th step of the previously described algorithm. In Step 1, it is necessary to solve $q^2$ equations with size $q \times q$. Since the complexity for solving a $q \times q$ equation is at most $q^3$ without any precomputation, the overall complexity for Step 1 is thus,

$$C(1) \le O(q^2 \cdot q^3) = O(n^{5/3}).$$

In Steps 2–4, $q$ Reed–Solomon codes of size $q^2$ will be decoded. Since the complexity in decoding Reed–Solomon codes is at most $O(n^2)$

$$C(2) + C(3) + C(4) \le qO((q^2)^2) = O(n^{5/3}).$$

Finally, its clear that

$$C(5) \le O(n).$$

Therefore, the overall decoding complexity is $O(n^{5/3})$.

Observe that in this decoding algorithm, it decodes in the same way whether only one symbol or all the $q$ symbols of $P_{i,0}, P_{i,1}, \ldots, P_{i,q-1}$, $i = 0, 1, \ldots, q^2 - 1$, are received wrong. Therefore, this decoding algorithm is capable of correcting more errors when burst errors occur. When errors occur randomly, this algorithm can still be applied, however, the number of errors that can be corrected could be much fewer.

Generally, the number of errors that can be corrected varies from

$$\left\lfloor \frac{k(q-1)-1}{2} \right\rfloor \text{ to } q\left(q^2 - k(0) + 1\right) = q\left(q^2 - \left\lfloor \frac{m}{q} - 1 \right\rfloor\right)$$

depending on the error locations.

## V. An Example

In this section, we will demonstrate the simple decoding procedures through an example. Let $q = 4$ and $m = 37$. Accordingly, the Hermitian curve is defined by the equation $y^4 + y = x^5$ over $\mathrm{GF}(4^2)$. From the discuss in Section II, we have $k(0) = 10, k(1) = 9, k(2) = 7, k(3) = 6$. Therefore, the parameters of $\mathrm{ERS}_{q^2}(k(0), q^2)$, $\mathrm{ERS}_{q^2}(k(1), q^2)$, $\mathrm{ERS}_{q^2}(k(2), q^2)$, and $\mathrm{ERS}_{q^2}(k(3), q^2)$ are $[16, 10, 7]$, $[16, 9, 8]$, $[16, 7, 10]$, and $[16, 6, 11]$, respectively. According to Theorem 1

$$\dim(\mathcal{H}_m) = k(0) + k(1) + k(2) + k(3) = 32, 27 \le \mathrm{dist}(\mathcal{H}_m) \le 28.$$

If a decoding algorithm as described in [9], [1], [3], [5], [4] are used, at most 13 errors can be corrected. Now we will use our decoding algorithm to correct a received word with 24 errors, which is completely impossible for any of the previously known Hermitian code decoding methods.

Since the solutions to $y^4 + y = 0$ are $\beta_0 = 0$, $\beta_1 = 1$, $\beta_2 = \alpha^5$, $\beta_3 = \alpha^{10}$, and $(1, \alpha)$ is a solution to (1), the 64 rational points can be represented as

$$P_{0,j} = (0, \beta_j),\ P_{i,j} = (\alpha^{i-1}, \alpha^{(i-1)(q+1)+1} + \beta_j), \quad i = 1, 2, \ldots, 15,\ j = 0, 1, 2, 3.$$

Consider a received vector

$$\boldsymbol{u} = (0, 0, 0, 0, \alpha, \alpha^2, \alpha^4, \alpha^5, \alpha^7, \alpha^9, \alpha^8, \alpha^6, 0, \ldots, 0, \alpha^5, \alpha^{10}, \alpha^4, \alpha, \alpha^{11}, \alpha^{13}, \alpha, \alpha^8, \alpha^6, \alpha^5, \alpha^{10}, \alpha^7, \alpha^{14}, \alpha^2, \alpha^3, 1, 0, 0, 0, 0)$$

where $\alpha^4 = \alpha + 1$. Now let us follow the procedures described in the previous algorithm to decode it.

$$\{(F(P_0), F(P_1), \ldots, F(P_{q^2-1})) \mid F(X_1, X_2) \in \mathrm{GF}(q)[X_1, X_2], \deg F(X_1, X_2) \le \tau\}$$

Step 1: Replace the transmitted codeword

$$\boldsymbol{c} = \Big(g(P_{0,0}), \ldots, g(P_{0,3}), \ldots, g(P_{15,0}), \ldots, g(P_{15,3})\Big)$$

with the previous $\boldsymbol{u}$. By solving the 16 four systems of equations (4), we get

$$\begin{aligned}
\boldsymbol{r}_3 &= (0, \alpha^4, \alpha^3, 0, \ldots, 0, 0, \alpha^2, \alpha^5, \alpha^2, 0)\\
\boldsymbol{r}_2 &= (0, \alpha^{14}, \alpha^{12}, 0, \ldots, 0, \alpha^4, \alpha^{12}, \alpha^{12}, \alpha^4, 0)\\
\boldsymbol{r}_1 &= (0, \alpha^5, \alpha^{13}, 0, \ldots, 0, \alpha, \alpha^7, \alpha^2, \alpha^5, 0)\\
\boldsymbol{r}_0 &= (0, \alpha^{10}, \alpha^{11}, 0, \ldots, 0, \alpha^{12}, \alpha^{12}, \alpha^3, \alpha^4, 0).
\end{aligned}$$

Step 2: Decode $\boldsymbol{r}_3$ in $\mathrm{ERS}_{q^2}(6, 16)$ using the decoding algorithm of extended Reed–Solomon codes [10], [11], we find the error vector

$$\boldsymbol{e}_3 = (0, \alpha^4, \alpha^3, 0, \ldots, 0, 0, \alpha^2, \alpha^5, \alpha^2, 0)$$

for $\boldsymbol{r}_3$, Therefore, the error locations are $E_2, E_3, E_{13}, E_{14}, E_{15}$.

Step 3: Replace the locations $E_2, E_3, E_{13}, E_{14}, E_{15}$ in $\boldsymbol{r}_2$ with "$\otimes$," we get the following vector:

$$(0, \otimes, \otimes, 0, \ldots, 0, \alpha, \otimes, \otimes, \otimes, 0).$$

Decode this vector $\mathrm{ERS}_{16}(7, 16)$, we find the error vector

$$\boldsymbol{e}_2 = (0, \alpha^{14}, \alpha^{12}, 0, \ldots, 0, \alpha^4, \alpha^{12}, \alpha^{12}, \alpha^4, 0)$$

with a new error location $E_{12}$.

Step 4: Repeat Step 3 for $\boldsymbol{r}_1$ and $\boldsymbol{r}_0$ in $\mathrm{ERS}_{16}(9, 16)$ and $\mathrm{ERS}_{16}(10, 16)$, respectively. We find the error vectors of

$$\begin{aligned}
\boldsymbol{e}_1 &= (0, \alpha^5, \alpha^{13}, 0, \ldots, 0, \alpha, \alpha^7, \alpha^2, \alpha^5, 0),\\
\boldsymbol{e}_0 &= (0, \alpha^{10}, \alpha^{11}, 0, \ldots, 0, \alpha^{12}, \alpha^{12}, \alpha^3, \alpha^4, 0).
\end{aligned}$$

In both cases, no new error locations are detected.

Step 5: Replace $(x_{j,0}, x_{j,1}, \ldots, x_{j,15})$ in the system of equations (4) with $\boldsymbol{e}_j$, $j = 0, 1, 2, 3$, and calculate the left-hand side, we get the error vector

$$\begin{aligned}
\boldsymbol{e} = (&0, 0, 0, 0, \alpha, \alpha^2, \alpha^4, \alpha^5, \alpha^7, \alpha^9, \alpha^8, \alpha^6, 0, \ldots, 0, \alpha^5, \alpha^{10}, \alpha^4,\\
&\alpha, \alpha^{11}, \alpha^{13}, \alpha, \alpha^8, \alpha^6, \alpha^5, \alpha^{10}, \alpha^7, \alpha^{14}, \alpha^2, \alpha^3, 1, 0, 0, 0, 0)
\end{aligned}$$

and, therefore, the transmitted codeword is

$$\boldsymbol{u} = (0, 0, 0, \ldots, 0, 0).$$

## VI. Discussion on Optimization of Hermitian Codes

*Generalized Reed–Muller* code [10] of order $\tau$ over $\mathrm{GF}(q)$ is defined as

$$\{(F(P_0), F(P_1), \ldots, F(P_{q^m-1})) \mid \deg F(X_0 X_1, \ldots, X_{m-1}) \le \tau\}$$

where $P_w$ runs through $\mathrm{GF}(q)^m$.

Now we will reformulate the above definition for $m = 2$ as the following proposition, which indicates that Hermitian code has a structure similar to the Reed–Muller code.

*Proposition 4:* A Reed–Muller code of order $\tau$ can be defined as the equation at the top of the page, where

$$F(x) = f_0(x) + y f_1(x) + \cdots + y^{\tau-1} f_{\tau-1}(x)$$

with $\deg f_{j_\tau} \le \tau - j_\tau, j_\tau = 0, 1, \ldots, \tau - 1$.

Proposition 4 shows that the Reed–Muller code and the Hermitian code have a similar structure. Their differences only lie in 1) the degrees of $f_j(x)$'s are different and 2) the $P_i$'s of the two codes are different. This observation stimulates us to design an optimized Hermitian code from two very possible approaches. One approach is to formulate different rules to control the degrees of $f_j(x)$'s, and the other approach is to select different rational points.

In fact, linear codes of the same form but with parameters better than Hermitian code and Reed–Muller code can be derived this way. Particularly, the Hermitian code can be optimized through selection of different Reed–Solomon codes for concatenation before direct sum.

## VII. Conclusion

In this correspondence, we proved that Hermitian code is a direct sum of concatenated Reed–Solomon codes over $\mathrm{GF}(q^2)$. Following this discovery, a decoding algorithm that is especially effective in combating burst errors was described. It was also pointed out that new optimized linear codes, which are either capable of correcting more errors, or being decoded at a lower complexity, can be constructed from Reed–Solomon codes. The optimization can be associated with the communication channels, however, further research still needs to be done.

## Acknowledgment

The author would like to thank the anonymous referees for their valuable comments.

## References

[1] G. L. Feng and T. R. N. Rao, "Decoding algebraic-geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 39, pp. 37–48, Jan. 1993.

[2] G. L. Feng, X. W. Wu, and T. R. N. Rao, "New double-byte error-correcting codes for memory systems," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1152–1163, Mar. 1998.

[3] J. Justesen, K. J. Larsen, H. E. Jensen, and T. Høholdt, "Construction and decoding of a class of algebraic geometry codes," *IEEE Trans. Inform. Theory*, vol. 35, pp. 811–821, July 1989.

[4] R. Pellikaan, "On a decoding algorithm for codes on maximal curves," *IEEE Trans. Inform. Theory*, vol. 35, pp. 1228–1232, Nov. 1989.

[5] A. N. Skorobogatov and S. G. Vlăduţ, "On a decoding of algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1051–1060, Sept. 1989.

[6] K. Yang and P. V. Kumar, "On the true minimum distance of Hermitian codes," in *Proc. Int. Workshop Coding Theory and Algebraic Geometry (Lecture Notes in Mathematics)*. Berlin, Germany: Springer-Verlag, 1991, vol. 1518, pp. 99–107.

[7] H. Stichtenoch, "A note on Hermitian codes over GF $(q^2)$," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1345–1348, Sept. 1988.

[8] H. J. Tiersma, "Remarks on codes from Hermitian curves," *IEEE Trans. Information Theory*, vol. IT–33, pp. 605–609, Sept. 1987.

[9] T. Yaghoobian and I. F. Blake, "Hermitian codes as generalized Reed-Solomon codes," *Des., Codes Cryptogr.*, vol. 2, pp. 5–17, 1992.

[10] F. J. MacWillams and N. J. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[11] S. Lin and D. Costello, *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ: Prentice Hall, 1983.