Designs, Codes and Cryptography (2021) 89:497–515
https://doi.org/10.1007/s10623-020-00836-6

Hermitian-lifted codes

Hiram H. López[1] · Beth Malmskog[2] · Gretchen L. Matthews[3] · Fernando Piñero-González[4] · Mary Wootters[5]

Received: 9 June 2020 / Accepted: 17 December 2020 / Published online: 12 January 2021

Abstract
In this paper, we construct codes for local recovery of erasures with high availability and constant-bounded rate from the Hermitian curve. These new codes, called Hermitian-lifted codes, are evaluation codes with evaluation set being the set of $\mathbb{F}_{q^2}$-rational points on the affine curve. The novelty is in terms of the functions to be evaluated; they are a special set of monomials which restrict to low degree polynomials on lines intersected with the Hermitian curve. As a result, the positions corresponding to points on any line through a given point act as a recovery set for the position corresponding to that point.

Keywords Hermitian curve · Codes with availability · Locally recoverable codes · Algebraic geometry codes · Lifted codes

Mathematics Subject Classification 94B05 · 11T71 · 94B27

1 Introduction

Let $\mathcal{C} \subset \mathbb{F}^n$ be a linear code of length n over a finite field $\mathbb{F}$. For a coordinate $i \in [n]$, we say that a set $R \subseteq [n]\backslash\{i\}$ is a *recovery set* for the index i in the code $\mathcal{C}$ if the i^{th} symbol c_i of a codeword $c \in \mathcal{C}$ can be recovered from the symbols $\left\{c_j \ : \ j \in R\right\}$. We say that $\mathcal{C}$ has

Communicated by J. W. P. Hirschfeld.

G. Matthews: Work partially supported by NSF DMS-1855136. M. Wootters: Work partially supported by NSF CAREER Award CCF-1844628, by CCF-BSF-1814629, and by a Sloan Research Fellowship.

✉ Hiram H. López
h.lopezvaldez@csuohio.edu

[1] Department of Mathematics and Statistics, Cleveland State University, Cleveland, OH, USA

[2] Department of Mathematics and Computer Science, Colorado College, Colorado Springs, CO, USA

[3] Department of Mathematics, Virginia Tech., Blacksburg, VA, USA

[4] Department of Mathematics, University of Puerto Rico in Ponce, Ponce, Puerto Rico, USA

[5] Departments of Computer Science and Electrical Engineering, Stanford University, Stanford, CA, USA

locality r and *availability* t if for each $i \in [n]$, there are t disjoint recovery sets for i in $\mathcal{C}$, each of size at most r.

Constructing codes with locality and availability is desirable for several reasons. Codes with extremely large availability, $t = \Omega(n)$, are known to be equivalent to *locally decodable codes* (LDCs) [10,19], which are objects of interest in theoretical computer science, complexity theory, and cryptography; see [22] for a survey. Codes with smaller availability, $t = O(1)$, have been studied recently in the context of *distributed storage:* if data is encoded and distributed over multiple nodes in a distributed system, then a small piece of data can be accessed efficiently by many users simultaneously. There are also variants on codes with locality and availability, such as *batch codes* and *PIR codes*, with applications in cryptography and private information retrieval; we refer the reader to the survey [18] for more details. Finally, codes with intermediate availability—where t is sublinear in n but still growing—have been studied as a bridge between the two settings above, and as an interesting problem in itself [12–14].

In this work we introduce a new type of *lifted code. Lifted codes* are a class of codes which have given rise to codes with good locality and intermediate availability. Lifted codes, introduced by Guo, Kopparty and Sudan [1], are evaluation codes of multivariate polynomials over large fields. The lift of a univariate evaluation code $\mathcal{C}_0$ to m variables is the evaluation code corresponding to the set of all m-variate polynomials whose restriction to every line corresponds to a codeword in $\mathcal{C}_0$. For example, the *lifted Reed-Solomon code* is the code corresponding to all m-variate polynomials whose restriction to every line is a low-degree univariate polynomial. Surprisingly, the set of all such polynomials can be much larger than the corresponding Reed-Muller code (corresponding to multivariate polynomials of small total degree) when the characteristic of the base field is small, and can even have rate approaching one [1]. Several variants of the lifting operation have been proposed, with the goal of making the construction more flexible, for example: working with different base codes [1,2,5]; including derivative information about the polynomials [14,20]; and only restricting to certain sets of lines [12].

In this paper we introduce a novel variant on the lifted code construction, by considering evaluation codes not on $\left(\mathbb{F}_q\right)^n$, but rather on the rational points of the Hermitian curve $\mathcal{H}_q$ over $\mathbb{F}_{q^2}$; that is, our code corresponds to all bivariate polynomials, evaluated on $\mathcal{H}_q$, so that the restriction to any line agrees with some low-degree univariate polynomial *on the points of* $\mathcal{H}_q$ *intersected with that line*. We call such a code a *Hermitian-Lifted Code*, because we are taking the lift with respect to a Hermitian curve.

For any even prime power q, Hermitian-lifted codes have length q^3 with locality q and availability q^2-1. Just as with the example of lifted Reed-Solomon codes mentioned above—and perhaps just as surprisingly—these codes have rate much larger than one would expect. More precisely, it is not hard to see that the code described above contains the one-point Hermitian code C_{q,q^2-1} (see below for notation); but this one-point code has rate that tends to 0 as q tends to infinity. Our main mathematical result is that in fact Hermitian-lifted codes have rate bounded below by a positive constant *independent* of q.

Evaluation codes on the points of geometric objects offer an elegant and flexible way to create codes with good parameters, bounded through geometry, with locality arising naturally from algebraic and geometric relationships. The rich structure of certain curves and their associated function fields enable a wide variety of geometric and algebraic perspectives that might create excellent codes. Our construction combines the extremely effective curve-centered approach that began in [6] and extended to locally recoverable codes in [3,11] with the lifting perspective of [1] to obtain novel codes which are not special cases of either approach.

In summary, our contributions are as follows. First, we introduce the notion of curve-lifted codes. This is a novel approach that combines ideas from curve-based codes and lifted codes in order to obtain good locally recoverable codes. Specifically, the evaluation points are simply rational points on the curve, as in the one-point code case, while the collection of functions to be evaluated is expanded to obtain a better code rate while guaranteeing locality and availability. We instantiate this idea by studying Hermitian-lifted codes. While Hermitian-lifted codes do offer good locality and availability, the quantitative parameters are not better than the existing state-of-the-art. Rather, we view the primary contribution of this work as introducing a new paradigm: we view our construction as a proof of concept that combining these two views can result in novel codes, providing an important addition to the literature and introducing an approach that could lead to new insights and may eventually improve the state-of-the-art.

Second, we provide a positive lower bound on the rate of Hermitian-lifted codes as $q \to \infty$. Such a bound is surprising, since the corresponding one-point Hermitian code has a rate that tends to zero as $q \to \infty$. Our approach is to study the set of "good" monomials whose restriction to any line, intersected with the Hermitian curve, agrees with a low-degree polynomial. We give a sufficient condition for a monomial to be good, and establish via a counting argument that there are many such monomials. This establishes a lower bound on the dimension of the code.

For the rest of the introduction, we review the Hermitian curve and related code constructions. The rest of the paper, after the Introduction, is organized as follows. Hermitian-lifted codes are introduced in Sect. 2, and information about their recovery sets is found there. The main theorem, providing the lower bound on the code rate, and proof are given in Sect. 3. Examples are given in Sects. 4 and 5 provides a brief conclusion.

1.1 The Hermitian curve and prior code constructions

An algebraic geometric perspective has proven useful in coding theory, particularly in the case of evaluation codes using the points of curves (dimension 1 varieties) defined over finite fields. These codes can be viewed as generalizations of Reed-Solomon codes, with the advantage that the length of the code is not bounded above by the field size, allowing for much longer codes with more codewords than a RS code over the same field. The length of the evaluation code is bounded by the number of points on the curve over the given field; thus curves with as many points as possible over a given field are useful in this context. The Hermitian curve is extremal among maximal curves and is almost certainly the best-studied maximal curve of positive genus.

1.1.1 The Hermitian curve

For a curve $\mathcal{X}$ defined over a field k and K/k any field extension, let $\mathcal{X}(K)$ denote the set of points on $\mathcal{X}$ defined over K. A curve's genus is a non-negative integer that is one measure of its complexity. The number of points possible for a curve over a finite field is limited by the Hasse-Weil bound of the curve's genus and the field size as follows: for a smooth, projective $\mathcal{X}$ of genus g defined over a finite field $\mathbb{F}_q$ of cardinality q, we have that

$$q + 1 - 2g\sqrt{q} \leq |\mathcal{X}(\mathbb{F}_q)| \leq q + 1 + 2g\sqrt{q}.$$

A curve which obtains the upper bound over a given field is said to be *maximal* over that field.

The Hermitian curve $\mathcal{H}_q$ is defined over $\mathbb{F}_q$ by the affine equation

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

This curve is smooth, irreducible, has genus $g = \frac{q(q-1)}{2}$, and has a single point at infinity, denoted by P_∞.

Let k be any natural number. We consider the points on $\mathcal{H}_q$ over the corresponding degree k extension field of $\mathbb{F}_q$, given explicitly by

$$\mathcal{H}_q(\mathbb{F}_{q^k}) = \{(x, y) \in \left(\mathbb{F}_{q^k}\right)^2 : x^q + x = y^{q+1}\} \cup \{P_\infty\}.$$

In this paper, we focus on the field $\mathbb{F}_{q^2}$. Note that $\mathcal{H}_q$ has $q^3 + 1$ points over $\mathbb{F}_{q^2}$, so $\mathcal{H}_q$ is maximal over $\mathbb{F}_{q^2}$.

The Hermitian curve $\mathcal{H}_q$ is extremal in many ways: it is the unique curve with the largest possible genus for a curve maximal over the field $\mathbb{F}_{q^2}$, and thus is the maximal curve with the largest number of points for that field. The curve is also as symmetrical as possible in that the automorphism group of H_q is PGU(3, q^2), which makes $\mathcal{H}_q$ the only curve of genus g with automorphism group of order greater than $16g^4$ [7].

This exceptional symmetry is apparent in the geometry of $\mathcal{H}_q$. The intersection of $\mathcal{H}_q$ with lines in the projective plane $\mathbb{P}^2$ will be very important to our construction.

Fact 1 *Every line in $\mathbb{P}^2$ that is not tangent to $\mathcal{H}_q$ intersects $\mathcal{H}_q$ in exactly $q+1$ distinct places. Tangent lines to $\mathcal{H}_q$ intersect $\mathcal{H}_q$ in exactly one place* [9].

We consider only lines defined over $\mathbb{F}_{q^2}$ which do not pass through the point P_∞, which can be parameterized by the affine equations $x = \alpha t + \beta$ and $y = t$ for $\alpha, \beta \in \mathbb{F}_{q^2}$. Note that each line tangent to $\mathcal{H}_q$ at an affine point does not pass through P_∞, so such a line is of the given form. Thus, for each P a point of $\mathcal{H}_q(\mathbb{F}_{q^2})\backslash\{P_\infty\}$, there are exactly $q^2 - 1$ distinct, non-tangent lines passing through P and q other affine points of the curve defined over $\mathbb{F}_{q^2}$.

1.1.2 Evaluation codes and one-point codes on Hermitian curves

V.D. Goppa first defined evaluation codes on curves over finite fields in the early 1980s [6]. The basic idea is to choose a set of points on the curve $\mathcal{X}$ as evaluation points, and a disjoint set of points as the support of a pole divisor. Codewords are created by evaluating functions which take on poles only in the support of the pole divisor on the evaluation points. The simplest case of Goppa's construction is a *one-point code*, where the pole divisor is $D = mP$ for some natural number m and P a point on $\mathcal{X}$. More concretely, we use the following definition.

Definition 1 Let $\mathcal{X}$ be a smooth curve defined over $\mathbb{F}_q$. Let P be a point on $\mathcal{X}(\mathbb{F}_q)$ and m be a natural number. Let $B = \{P_1, P_2, \ldots, P_n\}$ be a set of points in $\mathcal{X}(\mathbb{F}_q)$ not containing P, and let D be the divisor $D := P_1 + P_2 + \cdots + P_n$. Let $L(mP)$ be the Riemann-Roch space of functions on $\mathcal{X}$ with poles only at P of order at most m. The one-point code $C(D, mP)$ is the set $\{(f(P_1), f(P_2), \ldots f(P_n)) \in \left(\mathbb{F}_q\right)^n : f \in L(mP)\}$.

For simplicity, we define a one-point code on the Hermitian curve to take mP_∞ as the pole divisor. These codes have been well-studied, beginning with work by Tiersma [17] and Stichtenoth [16]. The Riemann-Roch space $L(mP_\infty)$ on $\mathcal{H}_q$ can be explicitly written down with basis

$$\{x^i y^j : 0 \leq j \leq q-1, iq + j(q+1) \leq m\}.$$

We use evaluation set $B = \mathcal{H}_q(\mathbb{F}_{q^2})\backslash\{P_\infty\}$, to obtain the evaluation divisor D. Adapting the notation of [4], we define the code $C_{q,m}$ to be one-point code $C(D, mP_\infty)$ with choices as above.

The length of $C_{q,m}$ is $n = q^3$. The dimension k of $C_{q,m}$ is given by $\dim(L(mP_\infty))$ for $m < q^3$ and k can be determined using the Riemann-Roch theorem. If $m > 2g - 2$ we have $k = \dim(L(mP_\infty)) = m - g + 1$; in general, $k = \dim(L(mP_\infty)) \geq m - g + 1$. The minimum distance d of the code can be bounded by $d \geq n - m$, since any function with a single pole of at most order m can have at most m zeros. The exact minimum distance has been determined for all values of m [8,21].

Evaluation codes with locality from algebraic curves appear in [3]. The authors define locally recoverable codes on curves, with locality arising from covering maps and recovery based on polynomial interpolation, and define a locally recoverable code with availability $t = 2$ on $\mathcal{H}_q$ by viewing the curve as a fiber product. In [11], the fiber product construction is utilized to define codes on curves with higher availability, with arbitrarily large availability possible for codes over large fields. A code of length q^3 on $\mathcal{H}_q$ is defined with availability $t = \frac{\log q}{\log p}$, where p is any prime and $q = p^t$. In this paper, we use an entirely different approach define codes of the same length on $\mathcal{H}_q$ (with q even) with vastly higher availability $t = q^2 - 1$.

1.1.3 Contrast of Hermitian-lifted codes with related literature

Hermitian-lifted codes have some similarities with constructions in the literature, but are distinct in a few important ways. The locally recoverable codes in [3] and [11] are based on fiber products of curves, an algebraic geometry construction which builds a curve $\mathcal{Y}$ by the product of several other curves $\mathcal{Y}_i$, $1 \leq i \leq t$, each with maps to a shared base curve $\mathcal{X}$. The functions evaluated in these codes are multivariate polynomials of bounded degree in each of the generators of the corresponding extensions of function fields. The t disjoint recovery sets in these codes correspond to fibers of the induced covering maps from $\mathcal{Y}$ to $\mathcal{Y}_i$. In Hermitian-lifted codes, the recovery sets correspond to the intersection points of the Hermitian curve with non-tangent lines. These could be viewed as the fibers of projection maps along each non-horizontal slope from $\mathcal{H}_q$ to a copy of the projective line $\mathbb{P}^1$, but these projection maps are not induced by a fiber product construction and there is not an obvious construction of the functions evaluated in Hermitian-lifted codes as any simple class of functions in the compositum of the function fields of the projective lines. For these codes to arise from the fiber product construction, we would need to construct the Hermitian curve $\mathcal{H}_q$ as a fiber product of q^2 projective lines. Each map $\mathcal{Y}_i \to \mathcal{X}$ would need to be degree $q + 1$, and could ramify above at most two points. By counting points, we see this could not lead to $\mathcal{H}_q$. Thus our construction creates a code which could not arise from the fiber product approach.

We also contrast Hermitian-lifted codes with other constructions based on lifted codes. Lifted codes and their variations [1,2,5,12,14,20] have provided constructions of codes with good locality and availability. It might be tempting to think that Hermitian-lifted codes are identical to bivariate lifts of Reed-Solomon codes, punctured to the Hermitian curve, but this is not the case. Indeed, Hermitian-lifted codes correspond to bivariate polynomials over $\mathbb{F}_{q^2}$ whose restriction to every line *intersected* with the Hermitian curve have degree at most $q-1$. The relevant lifted code, corresponding to bivariate polynomials whose restriction to every line has degree at most $q-1$, is known to be equal to the bivariate Reed-Muller code of degree $q - 1$ [15]. In particular, this code has dimension $O(q^2)$ and in particular the puncturing to the Hermitian code (of size q^3) has rate $O(\frac{1}{q})$. Thus, the Hermitian-lifted code is much larger than the corresponding lifted Reed-Solomon code, punctured to the Hermitian curve. We also note that Hermitian-lifted codes are different from the notions of lifted Hermitian codes given in [2,5]. The main difference is that in those works, the Hermitian code can be seen as the "base code," while in our work, the Hermitian code is used in the definition of the lifting process.

2 Code Construction

In this section, we give a few preliminary definitions and define Hermitian-lifted codes. For the rest of the paper, let $\mathcal{X} = \mathcal{H}_q(\mathbb{F}_{q^2})\backslash\{P_\infty\}$.

As discussed in the introduction, Hermitian-lifted codes are codes that are lifted with respect to Hermitian curves. More precisely, a Hermitian-lifted code is the evaluation code of all bivariate polynomials that agree with low-degree polynomials on all lines intersected with $\mathcal{X}$. We formalize this below.

First, we make the observation that one-point Hermitian codes are themselves naturally locally recoverable with locality q and availability $q^2 - 1$.

Observation 2 *The one-point code $C_{q,m}$ is locally recoverable with locality q and availability $q^2 - 1$ for all $m \leq q^2 - 1$.*

Proof Each index i of a position in $C_{q,m}$ corresponds to a point P_i in $\mathcal{H}_q(\mathbb{F}_{q^2})\backslash\{P_\infty\}$. For any $\alpha, \beta \in \mathbb{F}_{q^2}$, we define the function $L_{\alpha,\beta} : \mathbb{F}_{q^2} \to \left(\mathbb{F}_{q^2}\right)^2$ so that

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

For each such line $\mathrm{Im}(L_{\alpha,\beta})$ passing through P_i which is not tangent to $\mathcal{H}_q$ at P_i, let $R_{i,\alpha}$ be the set of indices corresponding to points in the set $(\mathcal{H}_q\left(\mathbb{F}_{q^2}\right) \cap \mathrm{Im}(L_{\alpha,\beta})\big) \backslash\{P_i\}$. We see that $|R_{i,\alpha}| = q$ and there are $q^2 - 1$ such mutually disjoint sets for each i.

Any codeword in $C_{q,m}$ is the evaluation of a function $f(x, y)$ which is a $\mathbb{F}_{q^2}$-linear combination of monomials of the form $x^a y^b$ where $b \leq q - 1$ and $aq + b(q + 1) \leq q^2 - 1$. Thus

$$a + b + b\frac{1}{q} \leq q - \frac{1}{q},$$

so

$$a + b \leq q - \frac{b+1}{q}.$$

Since a and b are non-negative integers, for each monomial in $f(x, y)$ we have $a+b \leq q-1$. Thus for all points on the line $\mathrm{Im}(L_{\alpha,\beta})$, the function f is identical to a univariate polynomial $g_\alpha(t)$ of degree at most $q - 1$.

If the symbol in position i of the codeword corresponding to f is erased, the value of $f(P_i)$ may be recovered by interpolating the polynomial $g_\alpha(t)$ from its values on the q points with indices in $R_{i,\alpha}$. □

It is worth noting that the one-point codes considered in Observation 2 have rate

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

as $q \to \infty$, where K denotes a canonical divisor on $\mathcal{H}_q$. In what follows, we develop Hermitian-lifted codes, which have rate bounded away from 0 as $q \to \infty$.

Definition 2 For polynomials $f \in \mathbb{F}_{q^2}[x, y]$ and $g \in \mathbb{F}_{q^2}[t]$, and for a function $L : \mathbb{F}_{q^2}[t] \to \mathbb{F}_{q^2}^2$, we say that $f \circ L$ *agrees with* g *on* $\mathcal{X}$ if $f(L(t)) = g(t)$ for all $t \in \mathbb{F}_{q^2}$ with $L(t) \in \mathcal{X}$.

Definition 3 Given a prime power q, let

$$\mathcal{F} = \left\{ f \in \mathbb{F}_{q^2}[x, y] \; : \; \begin{array}{l} \forall L \in \mathcal{L}, \exists g \in \mathbb{F}_{q^2}[t] \textit{ so that } \deg(g) \le q-1 \\ \textit{and so that } f \circ L \textit{ agrees with } g \textit{ on } \mathcal{X} \end{array} \right\},$$

where above

$$\mathcal{L} = \left\{ L_{\alpha,\beta} \; : \; \alpha \in \mathbb{F}_{q^2}, \beta \in \mathbb{F}_{q^2} \right\}$$

is the set of all lines of the form $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$.

Definition 4 (Hermitian-lifted codes) Let q be a prime power and let $\mathcal{F}$ be as in Definition 3. Define the *Hermitian-lifted code* $\mathcal{C} \subseteq \left(\mathbb{F}_{q^2}\right)^{q^3}$ as the evaluation code

$$\mathcal{C} = \left\{ (f(x, y))_{(x,y)\in\mathcal{X}} \; : \; f \in \mathcal{F} \right\}.$$

We note that $\mathcal{X}$, $\mathcal{F}$ and $\mathcal{C}$ depend on the choice of q; we suppress this in the notation since it will be clear from context. It is evident that $C_{q,m}$ is a subcode of $\mathcal{C}$.

Remark 1 *(Horizontal lines)* We ignore horizontal lines in our definition of $\mathcal{L}$ because they only intersect $\mathcal{X}$ in q affine places, rather than $q+1$. In particular, horizontal lines are different than non-horizontal lines because the point at ∞ is not an evaluation point in the code construction. As we see below, this will affect the locality of our resulting code.

It is easy to see (Observation 3 below) that Hermitian-lifted codes have locality and availability; the challenging task is to analyze the rate.

Observation 3 *Let q be any prime power, and let $\mathcal{C}$ be the Hermitian-lifted code as defined in Definition 4. Then $\mathcal{C}$ has locality q and availability $q^2 - 1$.*

Proof For any point $(x, y) \in \mathcal{X}$, there are $q^2 - 1$ lines $L_{\alpha,\beta}(t) \in \mathcal{L}$ that pass through (x, y), that are not tangent to $\mathcal{X}$, and that are not horizontal. Any two of these lines intersect only in the point (x, y), and each has q points on $\mathcal{X}$ other than (x, y). These q points form a repair group for the coordinate of $\mathcal{C}$ indexed by (x, y). Indeed, let $f \in \mathcal{F}$, and suppose that $L(t)$ is such a line. Let $t_0 \in \mathbb{F}_{q^2}$ be so that $L(t_0) = (x_0, y_0)$. As $f \in \mathcal{F}$, let $g(t)$ be a polynomial of degree at most $q-1$ so that $f(L(t)) = g(t)$ for any t so that $L(t) \in \mathcal{X}$. Given the q values

$$\{f(x, y) \; : \; (x, y) \in (\mathrm{Im}(L) \cap \mathcal{X})\backslash\{(x_0, y_0)\}\} = \left\{ g(t) \; : \; t \in \mathbb{F}_{q^2}\backslash\{t_0\} \right\}$$

of $f(x, y)$ on $(\mathrm{Im}(L) \cap \mathcal{X})\backslash\{(x_0, y_0)\}$, one can use Lagrange interpolation to recover the polynomial g, and hence $g(t_0) = f(L(t_0)) = f(x_0, y_0)$. Thus the symbol $f(x_0, y_0)$ of the codeword corresponding to f can be recovered by the q other symbols in the repair group corresponding to points in $(\mathrm{Im}(L) \cap \mathcal{X})\backslash\{(x_0, y_0)\}$. □

3 Main Theorem and Proof

Our main result is that Hermitian-lifted codes have rate bounded below by a constant independent of q. It is an immediate observation that $\mathcal{C}$ has rate at least $\frac{q(q+1)}{2q^3} \ge \frac{1}{2q}$, since C_{q,q^2-1} is a subcode of $\mathcal{C}$ and the dimension of C_{q,q^2-1} is $\frac{q(q+1)}{2}$. However, what may be surprising is that in fact there are many functions $f \in \mathcal{F}\backslash L\left((q^2-1)P_\infty\right)$, enough so that the rate of the code $\mathcal{C}$ is actually bounded below by a constant independent of q.

Theorem 4 *Suppose that $q \geq 4$ is a power of 2, and let $\mathcal{C}$ be as in Definition 4. Then the rate of $\mathcal{C}$ is at least* 0.007.

For the rest of this section, we will assume that $q = 2^\ell$ is a power of two, as in the hypotheses of Theorem 4. The strategy will be to find a large set of monomials $M_{a,b}(x, y) := x^a y^b$ for $a \leq q-1$ and $b \leq q^2 - 1$ so that $x^a y^b \in \mathcal{C}$.

It is not hard to see that such monomials lead to linearly independent codewords as shown in the next result.

Proposition 5 *Let $M_{a,b}(x, y) = x^a y^b$. Then the set of vectors*

$$\left\{ \left(M_{a,b}(x, y) \right)_{(x,y) \in \mathcal{X}} \, : \, 0 \leq a \leq q-1, 0 \leq b \leq q^2 - 1 \right\}$$

are linearly independent.

Proof The kernel of the evaluation map of the affine points of the Hermitian curve is generated by $y^{q+1} - x^q - x$, $y^{q^2} - y$, $x^{q^2} - x$. Under any monomial ordering where $y^{q+1} < x^q$, the polynomials $y^{q+1} - x^q - x$, $y^{q^2} - y$ are a Gröbner basis for the kernel. Hence the monomial set $M_{a,b}(x, y)$, $0 \leq a \leq q-1$, $0 \leq b \leq q^2 - 1$ can not contain any element from the kernel of the evaluation map, which implies the evaluations of $M_{a,b}$ are linearly independent. □

Since such monomials lead to linearly independent codewords by Proposition 5, bounding the number of them in $\mathcal{C}$ will give us a lower bound on the dimension of $\mathcal{C}$.

The proof proceeds in two steps. We give a brief overview below, after we introduce some necessary notation.

Definition 5 ($p_{\alpha,\beta}$, $\deg_{\alpha,\beta}$) Given $\alpha, \beta \in \mathbb{F}_{q^2}$, define

$$p_{\alpha,\beta}(t) := t^{q+1} + \alpha^q t^q + \alpha t + (\beta + \beta^q) = t^{q+1} + \alpha^q t^q + \alpha t + \gamma, \tag{1}$$

where above we are defining $\gamma := \beta + \beta^q$. For a polynomial $g(t) \in \mathbb{F}_{q^2}[t]$, let $\bar{g}(t)$ be the remainder obtained when $g(t)$ is divided by $p_{\alpha,\beta}(t)$, and define

$$\deg_{\alpha,\beta}(g) := \deg(\bar{g}_{\alpha,\beta}(t)).$$

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

To see why Definition 5 is relevant, consider a line $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$. Notice that $M_{a,b} \circ L_{\alpha,\beta}$ agrees with a polynomial g of degree strictly less than q on $\mathcal{X}$ if and only if

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

Indeed, write

$$(M_{a,b} \circ L_{\alpha,\beta})(t) = h(t) p_{\alpha,\beta}(t) + g(t)$$

for some polynomial $g(t)$ of degree at most q. Then for any t so that $L_{\alpha,\beta}(t) \in \mathcal{X}$, we have by definition that $t^{q+1} = (\alpha + \beta t)^q + \alpha + \beta t$, or in other words that $p_{\alpha,\beta}(t) = 0$. Thus, $M_{a,b} \circ L_{\alpha,\beta}$ agrees with $g(t)$ on $\mathcal{X}$, and since there are $q+1$ such values of t, $g(t)$ is the unique polynomial of degree at most q for which this is true.

We say that a monomial $M_{a,b}$ is **good** if for all lines $L_{\alpha,\beta} \in \mathcal{L}$,

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

The reasoning above leads to the following observation.

Observation 6 *If $M_{a,b}$ is good, then $M_{a,b} \in \mathcal{F}$.*

Thus, our goal will be to find a big set of good monomials. Our approach proceeds in two steps. In the first step (Sect. 3.1), we give a condition for when the monomial t^k has degree at most $q-1$ modulo $p_{\alpha,\beta}(t)$. In the second step (Sect. 3.2), we use this condition, along with Lucas' theorem, to show that there are many good monomials.

3.1 Behavior of monomials t^k modulo $p_{\alpha,\beta}(t)$

In this section, we give a condition on k for the monomial t^k to be low-degree modulo $p_{\alpha,\beta}(t)$ and prove Theorem 10 at the end of this section after we develop the necessary ingredients. Let α, β be elements of $\mathbb{F}_{q^2}$ such that the line $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$ is not tangent to the Hermitian curve $\mathcal{X}$. As α, β are fixed for the rest of this section, for notational convenience the polynomial $p_{\alpha,\beta}(t)$ will be denoted by $p(t)$ and $L_{\alpha,\beta}(t)$ will be denoted by $L(t)$. As in Definition 5, we let $\gamma := \beta + \beta^q$. Notice that $\gamma \in \mathbb{F}_q$.

Let $\sigma_0, \dots, \sigma_q$ be the roots of $p(t)$. There are $q+1$ distinct roots of $p(t)$ because there are $q+1$ distinct points in $\mathrm{Im}(L) \cap \mathcal{X}$. Thus

$$p(t) = t^{q+1} + \alpha^q t^q + \alpha t + \gamma = \prod_{i=0}^{q}(t - \sigma_i) = c_0 t^{q+1} + c_1 t^q + \cdots + c_q t + c_{q+1},$$

where $c_k = \sum_{S \subset \{0,\dots,q\}, |S|=k} \prod_{\ell \in S} \sigma_\ell$, for $k = 0, \dots, q$. In particular we have

$$c_0 = 1 \tag{2}$$

$$c_1 = \sum_{i=0}^{q} \sigma_i = \alpha^q \tag{3}$$

$$c_k = 0 \ \ \forall 1 < k < q \tag{4}$$

$$c_q = \sum_{i=0}^{q} \frac{\sigma_0 \cdots \sigma_q}{\sigma_i} = \alpha \tag{5}$$

$$c_{q+1} = \sigma_0 \cdots \sigma_q = \gamma. \tag{6}$$

For any $k \geq 0$ we define the element $P_k = \sum_{i=0}^{q} \sigma_i^k$. We show below that the values P_k provide a sufficient condition to guarantee $\deg_{\alpha,\beta}(t^k) < q$.

Proposition 7 *Let q be a power of 2 and let $\alpha, \beta \in \mathbb{F}_{q^2}$. Then $P_{k+1} = \alpha^q P_k$ if and only if $\deg_{\alpha,\beta}(t^k) < q$.*

Proof Write

$$t^k = g_k(t) p(t) + \bar{g}_k(t)$$

for some polynomial $g_k(t)$ so that the polynomial $\bar{g}_k(t)$ has degree at most q. Our goal is to show that $\deg(\bar{g}_k(t)) < q$ if and only if $P_{k+1} = \alpha^q P_k$.

As $\sigma_0, \dots, \sigma_q$ are the roots of $p(t)$, we have $\bar{g}_k(\sigma_i) = \sigma_i^k$. Thus, we know $q+1$ values of $\bar{g}_k$. Since $\bar{g}_k$ has degree less than q, we may use Lagrange interpolation to write

$$\bar{g}_k(t) = \sum_{i=0}^{q} \sigma_i^k \prod_{\ell \neq i} \left(\frac{t - \sigma_\ell}{\sigma_i - \sigma_\ell} \right) = \left(\sum_{i=1}^{q} \sigma_i^k \prod_{\ell \neq i} \frac{1}{\sigma_i - \sigma_\ell} \right) t^q + r(t),$$

where $\deg(r) < q$. Since

$$p(t) = t^{q+1} + \alpha^q t^q + \alpha t + \gamma = (t - \sigma_0) \cdots (t - \sigma_q),$$

taking the derivative of both sides yields

$$p'(t) = t^q + \alpha = \sum_{i=0}^{q} \prod_{\ell \neq i} (t - \sigma_\ell).$$

Thus,

$$p'(\sigma_i) = \sigma_i^q + \alpha = \prod_{\ell \neq i} (\sigma_i - \sigma_\ell).$$

Because σ_i is a root of $p(t)$, we have $\sigma_i^{q+1} + \alpha^q \sigma_i^q + \alpha \sigma_i = \gamma$; hence,

$$\left(\sigma_i^q + \alpha\right)\left(\sigma_i + \alpha^q\right) = \alpha^{q+1} + \gamma.$$

Thus, we get

$$\prod_{\ell \neq i} (\sigma_i - \sigma_\ell) = \frac{\alpha^{q+1} + \gamma}{\sigma_i + \alpha^q}.$$

As a consequence the coefficient of t^q in $\bar{g}_k(t)$ is given by

$$\sum_{i=1}^{q} \frac{\sigma_i^k (\sigma_i + \alpha^q)}{\alpha^{q+1} + \gamma} = \frac{P_{k+1} + \alpha^q P_k}{\alpha^{q+1} + \gamma}.$$

Thus, this coefficient is zero exactly when $P_{k+1} = \alpha^q P_k$, as desired. □

The goal now is to find k such that $P_{k+1} = \alpha P_k$. We begin with an observation about P_k for $0 \leq k < q$.

Lemma 8 *Let q be a power of 2. For $0 \leq k < q$, $P_k = \alpha^{qk}$ and $P_{kq} = \alpha^k$.*

Proof Since q is even, we have $P_0 = 1$. Take $1 \leq k < q$. Newton's identities imply that

$$kc_k = \sum_{i=1}^{k} (-1)^{i-1} c_{k-i} P_k,$$

and replacing the c_i with the values given in (2)-(6), we see that for $0 \leq k < q$, $P_k = \alpha^q P_{k-1}$. Thus $P_k = \alpha^{qk}$.

Because we are working over $\mathbb{F}_{q^2}$,

$$P_{kq} = \sum_{i=0}^{q} \sigma_i^{kq} = \left(\sum_{i=0}^{q} \sigma_i^k\right)^q = \left(\alpha^{qk}\right)^q = \alpha^k,$$

which completes the proof. □

We recall the *Kronecker product* of two matrices.

Definition 6 Let $A = [a_{ij}]$ be an $r \times s$ matrix and $B = [b_{ij}]$ an $m_1 \times m_2$ matrix. The Kronecker product of A and B is the $rm_1 \times sm_2$ matrix that can be expressed in block form as

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1s}B \\ a_{21}B & a_{22}B & \cdots & a_{2s}B \\ \vdots & \vdots & & \vdots \\ a_{r1}B & a_{r2}B & \cdots & a_{rs}B \end{pmatrix}.$$

Proposition 9 *Assume $q = 2^\ell$. Then*

$$\begin{pmatrix} P_0 & P_q & \cdots & P_{(q-1)q} \\ P_1 & P_{q+1} & \cdots & P_{(q-1)q+1} \\ \vdots & \vdots & & \vdots \\ P_{q-1} & P_{2q-1} & \cdots & P_{q^2-1} \end{pmatrix} = \begin{pmatrix} 1 & \alpha^{2^{\ell-1}} \\ \alpha^{(2^{\ell-1})q} & \gamma^{2^{\ell-1}} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & \alpha^2 \\ \alpha^{2q} & \gamma^2 \end{pmatrix} \otimes \begin{pmatrix} 1 & \alpha \\ \alpha^q & \gamma \end{pmatrix}.$$

Proof Denote by Γ_q the matrix of the left side and by Γ'_q the matrix of the right side of the proposed equality. For a root σ of $p(t) = t^{q+1} + \alpha^q t^q + \alpha t + \gamma$, $\sigma^k = \alpha^q \sigma^{k-1} + \alpha \sigma^{k-q} + \gamma \sigma^{k-q-1}$ for $k \geq q+1$. Thus we obtain that the P_k values satisfy the recurrence relation

$$P_k = \alpha^q P_{k-1} + \alpha P_{k-q} + \gamma P_{k-q-1}. \tag{7}$$

As a consequence, the (i, j) entry on the matrix Γ_q depends on the $(i-1, j)$, $(i, j-1)$, $(i-1, j-1)$ entries of Γ_q. This implies that the matrix Γ_q is fully determined by its first row and its first column. It is clear that the first row of Γ'_q is $(1, \alpha, \ldots, \alpha^q)$ and the first column of Γ'_q is $(1, \alpha^q, \ldots, \alpha^{q(q-1)})^T$. Moreover, Lemma 8 implies that the same is true for Γ_q; thus the first rows and first columns of Γ_q and Γ'_q are the same. In order to show that $\Gamma_q = \Gamma'_q$, we just need to verify that matrix Γ'_q satisfies (7). It is equivalent to show that every 2×2 block M of Γ'_q satisfies the relation

$$M_{22} = \alpha^q M_{12} + \alpha M_{21} + \gamma M_{11}. \tag{8}$$

We proceed by induction. It is clear that the matrix $\begin{pmatrix} 1 & \alpha \\ \alpha^q & \gamma \end{pmatrix}$ satisfies (8). Let $i > 1$ and assume that every 2×2 block of the matrix

$$B = \begin{pmatrix} 1 & \alpha^{2^{i-1}} \\ \alpha^{(2^{i-1})q} & \gamma^{2^{i-1}} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & \alpha^2 \\ \alpha^{2q} & \gamma^2 \end{pmatrix} \otimes \begin{pmatrix} 1 & \alpha \\ \alpha^q & \gamma \end{pmatrix}$$

satisfies (8). We will show that the matrix $\begin{pmatrix} 1 & \alpha^{2^i} \\ \alpha^{(2^i)q} & \gamma^{2^i} \end{pmatrix} \otimes B$ satisfies (8). Observe that the first row, first column, last row and last column of B are as shown:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{2^i-1} \\ \alpha^q & & & & \alpha^{2^i-2}\gamma \\ \alpha^{2q} & & & & \alpha^{2^i-3}\gamma^2 \\ \vdots & & & & \vdots \\ \alpha^{(2^i-1)q} & \alpha^{(2^i-2)q}\gamma & \alpha^{(2^i-3)q}\gamma^2 & \ldots & \gamma^{2^i-1} \end{pmatrix}. \tag{9}$$

Now it is straightforward to check that the matrix $\begin{pmatrix} 1 & \alpha^{2^i} \\ \alpha^{(2^i)q} & \gamma^{2^i} \end{pmatrix} \otimes B = \left(\begin{array}{c|c} B & \alpha^{2^i} B \\ \hline \alpha^{(2^i)q} B & \gamma^{2^i} B \end{array}\right)$ satisfies the desired property (8). Indeed, take any 2×2 block M. If M belongs to any of the four blocks $B, \alpha^{2^i} B, \alpha^{(2^i)q} B$ or $\gamma^{2^i} B$, then we are finished by induction. Otherwise, we have the following five cases:

(i) When M intersects the blocks B and $\alpha^{2^i} B$, $M = \begin{pmatrix} \alpha^{2^i - j}\gamma^{j-1} & \alpha^{2^i}\alpha^{jq} \\ \alpha^{2^i-(j+1)}\gamma^j & \alpha^{2^i}\alpha^{(j+1)q} \end{pmatrix}$ for some j.

(ii) When M intersects the blocks B and $\alpha^{(2^i)q} B$, $M = \begin{pmatrix} \alpha^{(2^i-j)q}\gamma^{j-1} & \alpha^{(2^i-(j+1))q}\gamma^j \\ \alpha^j \alpha^{(2^i)q} & \alpha^{j+1}\alpha^{(2^i)q} \end{pmatrix}$ for some j.

(iii) When M intersects the blocks $\alpha^{2^i} B$ and $\gamma^{2^i} B$, $M = \begin{pmatrix} \alpha^{2^i}\alpha^{(2^i-j)q}\gamma^{j-1} & \alpha^{2^i}\alpha^{(2^i-(j+1))q}\gamma^j \\ \alpha^j\gamma^{2^i} & \alpha^{j+1}\gamma^{2^i} \end{pmatrix}$ for some j.

(iv) When M intersects the blocks $\alpha^{(2^i)q} B$ and $\gamma^{2^i} B$, $M = \begin{pmatrix} \alpha^{(2^i)q}\alpha^{2^i-j}\gamma^{j-1} & \gamma^{2^i}\alpha^{jq} \\ \alpha^{(2^i)q}\alpha^{2^i-(j+1)}\gamma^j & \gamma^{2^i}\alpha^{(j+1)q} \end{pmatrix}$ for some j.

(v) When M intersects the four blocks—that is, M is the 2×2 matrix in the center—we have $M = \begin{pmatrix} \gamma^{2^i-1} & \alpha^{2^i}\alpha^{(2^i-1)q} \\ \alpha^{(2^i)q}\alpha^{2^i-1} & \gamma^{2^i} \end{pmatrix}$.

It is not hard to check that in all five cases, we have $M_{22} = \alpha^q M_{12} + \alpha M_{21} + \gamma M_{11}$. □

Finally, we are ready to prove Theorem 10, stated below, which provides a sufficient condition for $\deg_{\alpha,\beta}(t^k) < q$.

Theorem 10 *Assume $q = 2^\ell$. Let $0 \leq k < q^2$, and write $k = wq + z$ where $z < q$. Let $\alpha, \beta \in \mathbb{F}_{q^2}$. Suppose that either $w = 0$, or that there exists $1 \leq i \leq \ell$ such that $w \equiv 0 \mod 2^i$ and $z \not\equiv -1 \mod 2^i$. Then $\deg_{\alpha,\beta}(t^k) < q$.*

Proof of Theorem 10 Suppose that $k = wq + z$ as in the theorem statement. By Proposition 7, we just need to check that $P_{k+1} = \alpha^q P_k$. When $w = 0$, it is clear that $P_{k+1} = \alpha^q P_k$ because by Lemma 8, for $0 \leq k \leq q$, $P_k = \alpha^{qk}$.

Suppose that there exists an i so that $w \equiv 0 \mod 2^i$ and $z \not\equiv -1 \mod 2^i$. Then let

$$A = \begin{pmatrix} 1 & \alpha^{2^{\ell-1}} \\ \alpha^{(2^{\ell-1})q} & \gamma^{2^{\ell-1}} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & \alpha^{2^i} \\ \alpha^{(2^i)q} & \gamma^{2^i} \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & \alpha^{2^{i-1}} \\ \alpha^{(2^{i-1})q} & \gamma^{2^{i-1}} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 & \alpha \\ \alpha^q & \gamma \end{pmatrix},$$

so that $A \in \mathbb{F}_{q^2}^{2^{\ell-i} \times 2^{\ell-i}}$ and $B \in \mathbb{F}_{q^2}^{2^i \times 2^i}$. By Proposition 9

$$\begin{pmatrix} P_0 & P_q & \cdots & P_{(q-1)q} \\ P_1 & P_{q+1} & \cdots & P_{(q-1)q+1} \\ \vdots & \vdots & & \vdots \\ P_{q-1} & P_{2q-1} & \cdots & P_{q^2-1} \end{pmatrix} = A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1s}B \\ a_{21}B & a_{22}B & \cdots & a_{2s}B \\ \vdots & \vdots & & \vdots \\ a_{s1}B & a_{s2}B & \cdots & a_{ss}B \end{pmatrix}$$

where $s = 2^{\ell-i}$. Suppose that P^k lies in the block $a_{cd}B$ for some $c, d \in \{1, \ldots, 2^{\ell-i}\}$. The fact that $w \equiv 0 \mod 2^i$ means that the element P_k is in the first column of the block $a_{cd}B$. The fact that $z \not\equiv -1 \mod 2^i$ means that P_k is not in the last row of the block $a_{cd}B$. In particular, P_{k+1} is also in the block $a_{cd}B$. Because of the structure of the first column of B, shown in (9), we have $P_{k+1} = \alpha^q P_k$. Thus by Proposition 7, we have $\deg_{\alpha,\beta}(t^k) < q$. □

3.2 Bound on the rate of the code

In this section we use Theorem 10 in order to bound the rate of our code construction below, completing the proof of Theorem 4.

As discussed above, the strategy will be to find a large set of monomials $M_{a,b}(x, y) = x^a y^b$ for $a \leq q - 1$ and $b \leq q^2 - 1$ so that $M_{a,b}$ is good, and hence, by Observation 6, $M_{a,b} \in \mathcal{F}$. Since such monomials lead to linearly independent codewords by Proposition 5, this will give us a lower bound on the dimension of $\mathcal{C}$.

If $a + b < q$, then clearly $M_{a,b}$ is good. Indeed, in this case $\deg(M_{a,b} \circ L_{\alpha,\beta}) < q$ for all α, β, and so reducing modulo $p_{\alpha,\beta}$ does not change this.

If $a + b \geq q$, there are two mechanisms that contribute to $M_{a,b}(x, y)$ being good. To see this, we may expand $M_{a,b} \circ L_{\alpha,\beta}$ as follows:

$$(M_{a,b} \circ L_{\alpha,\beta})(t) = M_{a,b}(\alpha t + \beta, t) = (\alpha t + \beta)^a t^b = \sum_{j \leq a} \binom{a}{j} \alpha^j \beta^{a-j} t^{b+j}. \tag{10}$$

The first mechanism that can contribute to the goodness of $M_{a,b}$ is that the terms t^{b+j} in (10) could have small degree mod $p_{\alpha,\beta}(t)$, such as per Theorem 10. The second mechanism is that the binomial coefficients $\binom{a}{j}$ could vanish mod 2. To understand this second mechanism, we will use Lucas' Theorem, stated below.

Definition 7 Let a and b be integers between 0 and $2^d - 1$, and let $\text{bin}(a) \in \{0, 1\}^d$ denote the binary expansion of a. We say that a **lies in the 2-shadow of** b, denoted $a \leq_2 b$, if

$$\text{Supp}(\text{bin}(a)) \subseteq \text{Supp}(\text{bin}(b)).$$

Theorem 11 (Lucas) *Let $0 \leq a \leq b$ be integers. Then $\binom{b}{a}$ is zero mod 2 if and only if $a \not\leq_2 b$, meaning a does not lie in the 2-shadow of b.*

Before continuing, we give an example to illustrate how both mechanisms come into play.

Example 1 Let $q = 4$ and consider $M_{2,8}(x, y) = x^2 y^8$. This is a high-degree polynomial on the curve $\mathcal{X}$. However, on every line $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$, we have

$$\begin{aligned} M_{2,8}(L_{\alpha,\beta}(t)) &= (\alpha t + \beta)^2 t^8 \\ &= (\alpha^2 t^2 + \beta^2) t^8 \\ &= \alpha^2 t^{10} + \beta^2 t^8. \end{aligned}$$

In the second line above when the cross-terms $\beta \alpha t + \beta \alpha t = 0$ canceled, Lucas' theorem was in action, as the binomial coefficient $\binom{2}{1}$ vanishes. Now in the third line, we are left with the two monomials t^{10} and t^8. By Theorem 10, both of these reduce to something of degree less than q. Indeed, we have $10 = 2 + 2 \cdot q$. As $2 \equiv 0 \mod 2$ and $2 \not\equiv -1 \mod 2$, we have $\deg_{\alpha,\beta}(t^{10}) < q$. We have that $8 = 0 + 2 \cdot q$. As $0 \equiv 0 \mod 2$ and $2 \not\equiv -1 \mod 2$, we obtain $\deg_{\alpha,\beta}(t^8) < q$. We conclude that $\deg_{\alpha,\beta}(M_{2,8}(L_{\alpha,\beta}(t))) < q$, and hence $M_{2,8}$ is good.

Notice that both mechanisms were important here. In particular, if the binomial coefficient $\binom{2}{1}$ had not disappeared, we would be left with a term t^9. One can check that $\deg_{\alpha,\beta}(t^9) = 4$ for some α, β, and so this would result in a t^4 term in $(M_{2,8} \circ L_{\alpha,\beta})(t) \mod p_{\alpha,\beta}(t)$ and $M_{a,b}$ would not be good.

Finally, we can prove our main theorem, Theorem 4, which says that the rate of a Hermitian-lifted code is bounded below by a positive constant.

Proof of Theorem 4 As per Observation 6, we will come up with a large set of monomials $M_{a,b}$ that are good. By Proposition 5, the resulting codewords are linearly independent, and this will yield a lower bound on the dimension of $\mathcal{C}$.

Let $q = 2^\ell$ as in the theorem statement. Below, for an integer x, write $x = \sum_r x_r 2^r$, so that x_r denotes the r'th least significant bit in the binary expansion of x.

Claim 12 *Suppose that $a \le q-1$ and $b \le q^2-1$ satisfy the following properties.*

(i) $b = wq + b'$ for some $w < q$ and some $b' < 2^{\ell-1}$, so that $w \equiv 0 \mod 2^i$ for some $1 \le i \le \ell$;
(ii) $a < 2^{\ell-1}$;
(iii) there is some $0 \le s \le i-1$ so that $a_s = b'_s = 0$.

Then $M_{a,b}$ is good.

Proof Suppose that a, b satisfy (i)-(iii). Let $L_{\alpha,\beta}(t) = (\alpha t + \beta, t)$ be a line in $\mathcal{L}$ and write

$$(M_{a,b} \circ L_{\alpha,\beta})(t) = \sum_{j \le a} \binom{a}{j} \alpha^j \beta^{a-j} t^{j+b} = \sum_{j \le_2 a} \alpha^j \beta^{a-j} t^{j+b} \tag{11}$$

using Lucas' theorem in the second equality. Notice that for any $j \le_2 a$, we have $j < 2^{\ell-1}$ and $j_s = 0$, using properties (ii) and (iii). Then the only monomials that appear in (11) are of the form t^k where $k = wq + b' + j$ for w, b' as in (i) and for $j \le_2 a$. Let i be as in (i), so that $w \equiv 0 \mod 2^i$. We claim that $b' + j \not\equiv -1 \mod 2^i$. Indeed, we can write

$$b' = 2^{s+1} b'' + b''' \qquad \text{and } j = 2^{s+1} j'' + j'''$$

for some $b''', j''' < 2^s$, using the fact that $b'_s = j_s = 0$. Note that there exists some $c \le 2^i - 2^{s+1}$ so that

$$2^{s+1}(b'' + j'') \equiv c \mod 2^i.$$

(Indeed, this is true for any integer multiple of 2^{s+1}.) Thus,

$$b' + j \equiv c + b''' + j''' \mod 2^i.$$

Since $b''', j''' < 2^s$, we have

$$c + b''' + j''' < (2^i - 2^{s+1}) + (2^{s+1} - 1) = 2^i - 1,$$

which means that $b' + j \not\equiv -1 \mod 2^i$, as claimed.

Thus, k is of the form $k = wq + z$ (where $z = b' + j$) so that $w \equiv 0 \mod 2^i$ and $z \not\equiv -1 \mod 2^i$. By Theorem 10, $\deg_{\alpha,\beta}(t^k) < q$. Since this is true for every power t^k that appears in (11), $\deg_{\alpha,\beta}(M_{a,b} \circ L_{\alpha,\beta}) < q$ for all α, β, and hence $M_{a,b}$ is good. □

Finally, we count the number of pairs a, b meeting the description in Claim 12. We iterate over all s, where we take s to be the smallest index so that $a_s = b'_s = 0$. For a given s, there are $4^s - 3^s$ ways to assign the bits $a_0, \ldots, a_{s-1}$ and $b'_0, \ldots, b'_{s-1}$, since there are only 3^s ways to never have $a_r = b'_r = 0$ for any $0 \le r \le s-1$. Then there are $4^{\ell-s-2}$ ways to assign the bits $a_{s+1}, \ldots, a_{\ell-2}, b'_{s+1}, \ldots, b'_{\ell-2}$. Finally, there are $2^{\ell-s-1}$ ways to assign the bits $w_{s+1}, \ldots, w_{\ell-1}$. Notice that we will choose $w_0, \ldots, w_s = 0$, ensuring that $w \equiv 0 \mod 2^{s+1}$ and in particular $w \equiv 0 \mod 2^i$ for some $i > s$.

Thus, the total number of monomials meeting the description in Claim 12 is

$$\begin{aligned}\sum_{s=0}^{\ell-1}\left(4^s-3^s\right)4^{\ell-s-2}2^{\ell-s-1} &= \frac{2^{3\ell}}{32}\sum_{s=0}^{\ell-1}\left(4^s-3^s\right)8^{-s}\\ &= \frac{2^{3\ell}}{32}\cdot\frac{2}{5}\left(1+4\left(\frac{3}{8}\right)^{\ell}-5\left(\frac{1}{2}\right)^{\ell}\right)\\ &\geq 0.007\cdot q^3\end{aligned}$$

using the fact that $q=2^{\ell}$ and the assumption that $\ell\geq 2$. Since the length of $\mathcal{C}$ is $q^3=|\mathcal{X}|$, this implies that the rate of $\mathcal{C}$ is at least 0.007. □

We note that Claim 12 does not take into account all of the good monomials; in particular, $M_{a,b}$ with $a=b=2^{\ell-1}-1$ is a good monomial that is not covered. In the examples in Sect. 4, we see higher rates.

We conclude this section about the rate of the code with a very loose bound on another parameter, namely the minimum distance.

Proposition 13 *The minimum distance d of the code $\mathcal{C}$ is bounded by $q^2\leq d\leq q^3-q^2+1$.*

Proof The upper bound given by the fact that C_{q,q^2-1} is contained in $\mathcal{C}$, and the minimum distance of C_{q,q^2-1} is given in Theorem 5 of [16]. The lower bound is based on our recovery procedure. If V is a codeword with a non-zero symbol in position i, this corresponds to a function f_V which is non-zero on the point P_i. Position i has q^2-1 disjoint recovery sets, and for each recovery set, at least one symbol in V must be non-zero (since the zero polynomial will be interpolated if all symbols in the recovery set positions are zero). Thus any codeword with any non-zero symbol must have non-zero symbols in at least q^2 positions. □

4 Examples

In computed examples, the actual code $\mathcal{C}$ has rate much higher than the asymptotic lower bound computed in Sect. 3.2. The following examples illustrate how much higher.

4.1 The code $\mathcal{C}$ when $q=4$

When $q=4$, we work with the Hermitian curve $x^4+x=y^5$, which has 65 points over $\mathbb{F}_{16}$ including one point at infinity, giving a code of length $n=64$. The code $\mathcal{C}$ has dimension 13, with basis the set of monomials $x^a y^b$ where

$$\begin{aligned}(a,b)\in\ &\{(0,0),(0,1),(0,2),(0,3),(0,8),(0,10),(1,0),(1,1),(1,2),(2,0),(2,1),\\ &(2,8),(3,0)\}.\end{aligned}$$

These exponent pairs are plotted in Fig. 1. In contrast, the comparable non-lifted one-point Hermitian code $C_{4,15}$ has dimension 10. Thus the rate of $\mathcal{C}$ is $\frac{13}{64}\approx 0.20$, while the rate of $C_{4,15}$ is $\frac{10}{64}\approx 0.16$.

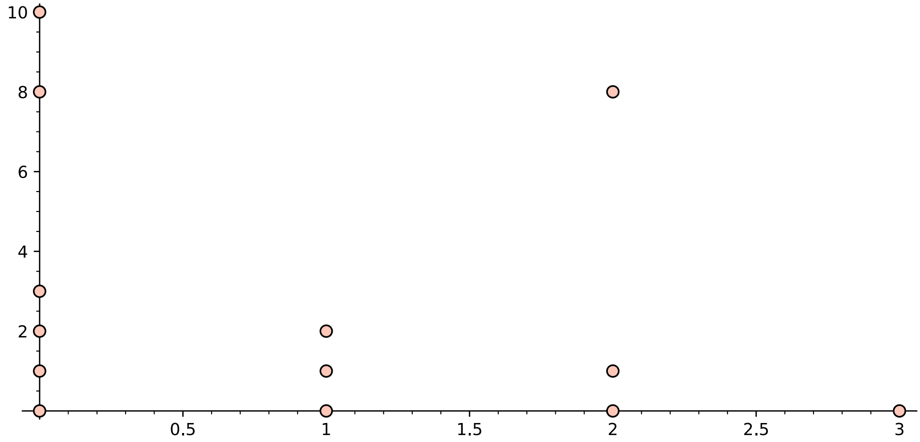

Fig. 1 Exponent pairs (a, b) with $x^a y^b \in \mathcal{C}$ for $q = 4$ (a is on horizontal axis)

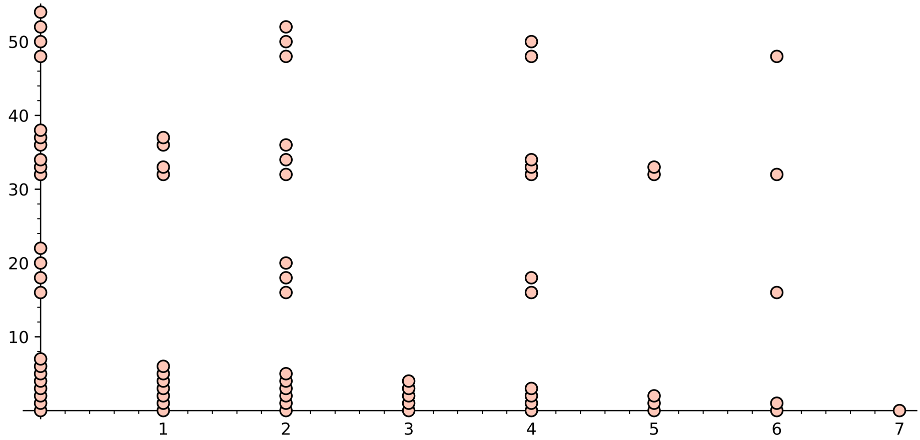

Fig. 2 Exponent pairs (a, b) with $x^a y^b \in \mathcal{C}$ for $q = 8$ (a is on horizontal axis)

4.2 The code $\mathcal{C}$ when $q = 8$

When $q = 8$, we work with the Hermitian curve $x^8 + x = y^9$, which has 513 points over $\mathbb{F}_{64}$ including one point at infinity, giving a code of length $n = 512$. The code $\mathcal{C}$ has dimension 75, with basis the set of monomials $x^a y^b$ where

$$\begin{aligned}(a, b) \in \{&(0, 0), (0, 1), (0, 2), (0, 3), (0, 4), (0, 5), (0, 6), (0, 7), (0, 16), (0, 18), (0, 20),\\ &(0, 22), (0, 32), (0, 33), (0, 34), (0, 36), (0, 37), (0, 38), (0, 48), (0, 50), (0, 52),\\ &(0, 54), (1, 0), (1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (1, 32), (1, 33), (1, 36),\\ &(1, 37), (2, 0), (2, 1), (2, 2), (2, 3), (2, 4), (2, 5), (2, 16), (2, 18), (2, 20),\\ &(2, 32), (2, 34), (2, 36), (2, 48), (2, 50), (2, 52),\\ &(3, 0), (3, 1), (3, 2), (3, 3), (3, 4), (4, 0),\\ &(4, 1), (4, 2), (4, 3), (4, 16), (4, 18), (4, 32), (4, 33), (4, 34), (4, 48), (4, 50),\end{aligned}$$

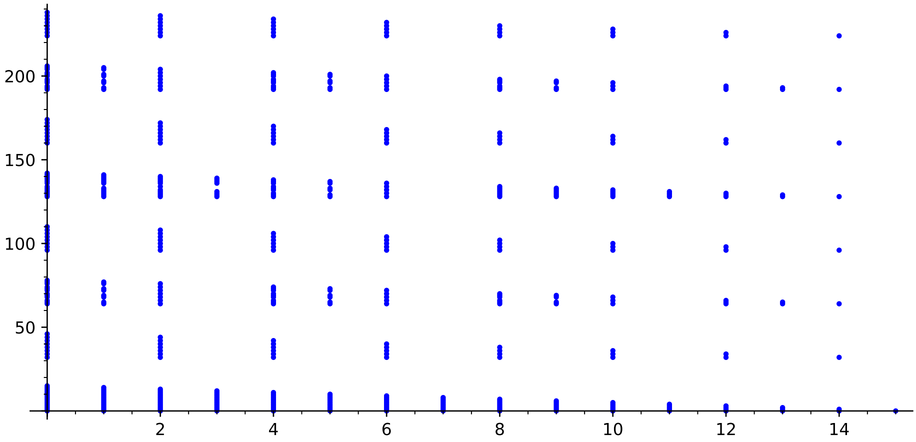

Fig. 3 Exponent pairs (a, b) with $x^a y^b \in \mathcal{C}$ for $q = 16$ (a is on horizontal axis)

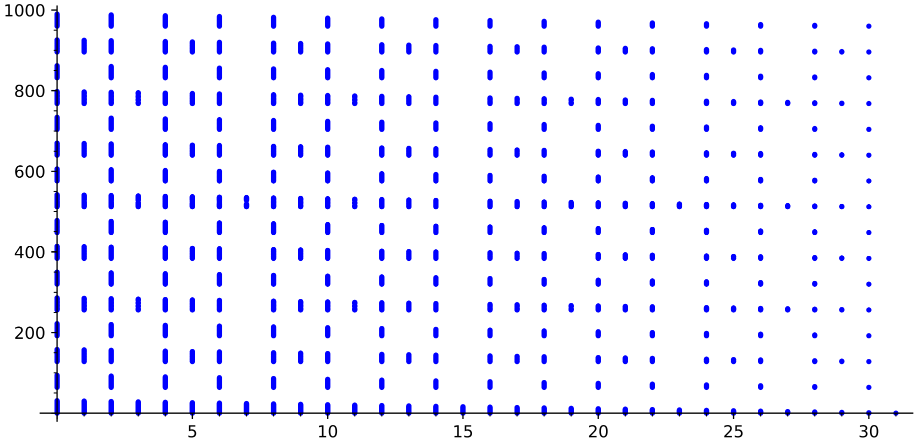

Fig. 4 Exponent pairs (a, b) with $x^a y^b \in \mathcal{C}$ for $q = 32$ (a is on horizontal axis)

$$(5, 0), (5, 1), (5, 2), (5, 32), (5, 33),$$
$$(6, 0), (6, 1), (6, 16), (6, 32), (6, 48), (7, 0)\}.$$

These exponent pairs are plotted in Fig. 2. In contrast, the comparable non-lifted one-point Hermitian code $C_{8,63}$ has dimension 36. Thus the rate of $\mathcal{C}$ is $\frac{75}{512} \approx 0.15$. The rate of $C_{8,63}$ is $\frac{36}{512} \approx 0.07$.

4.3 The code $\mathcal{C}$ when $q = 16$

When $q = 16$, we work with the Hermitian curve $x^{16} + x = y^{17}$, which has 4097 points over $\mathbb{F}_{256}$ including one point at infinity, giving a code of length $n = 4096$. The code $\mathcal{C}$ has dimension 505, with basis the set of monomials $x^a y^b$ where (a, b) are as depicted in Fig. 3. In contrast, the comparable non-lifted one-point Hermitian code $C_{16,255}$ has dimension 136. Thus the rate of $\mathcal{C}$ is $\frac{505}{4096} \approx 0.123$. The rate of $C_{16,255}$ is $\frac{136}{4096} \approx 0.033$.

4.4 The code $\mathcal{C}$ when $q = 32$

When $q = 32$, we work with the Hermitian curve $x^{32} + x = y^{33}$, which has 32,769 points over $\mathbb{F}_{256}$ including one point at infinity, giving a code of length $n = 32,768$. The code $\mathcal{C}$ has dimension 3675, with basis the set of monomials $x^a y^b$ where (a, b) are as depicted in Fig. 4. In contrast, the comparable non-lifted one-point Hermitian code $C_{32,1025}$ has dimension 528. Thus the rate of $\mathcal{C}$ is $\frac{3675}{32768} \approx 0.112$. The rate of $C_{32,1025}$ is $\frac{528}{32768} \approx 0.016$.

5 Conclusion

In this paper, we define Hermitian-lifted codes, which are codes defined on the Hermitian curve with small locality, high availability, and rate bounded below by a constant. They are the evaluation code of polynomials whose restrictions to lines, intersected with the Hermitian curve, are all low-degree. We study these codes as a first example of curve-lifted codes. We establish the lower bound on the rate via a counting argument applied to certain "good" monomials.

We conclude with a few open questions. First, it is an interesting question to completely characterize the "good" monomials for Hermitian-lifted codes; determining their number would pin down the rate of these codes. Second, it is interesting to explore other constructions of curve-lifted codes. We view one of the main contributions of this work as introducing this paradigm for code constructions, and it is our hope that our construction and analysis of Hermitian-lifted codes may serve as a prototype for the construction and analysis of other families of curve-lifted codes.

Acknowledgements The authors thank American Institute of Mathematics (AIM) for hosting this collaboration through its SQuaREs program.

References

1. Alan G., Swastik K., Madhu S.: New affine-invariant codes from lifting. In: Innovations in Theoretical Computer Science, ITCS '13, Berkeley, CA, USA, January 9–12, 2013, pp. 529–540 (2013).
2. Alan G.: High-rate locally correctable codes via lifting. IEEE Trans. Inf. Theory **62**(12), 6672–6682 (2015).
3. Alexander B., Itzhak T., Serge V.: Locally recoverable codes on algebraic curves. IEEE Trans. Inf. Theory **63**(8), 4928–4939 (2017).
4. Edoardo B., Alberto R.: On the geometry of Hermitian one-point codes. J. Algebra **397**, 499–514 (2014).
5. Eli B.S., Ariel G., Yohay K., Swastik K., Shubangi S.: A new family of locally correctable codes based on degree-lifted algebraic geometry codes. In: Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing, pp. 833–842 (2013).
6. Goppa V.D.: Algebraico-geometric codes. Math. USSR Izv. **21**, 75–91 (1983).
7. Henning S.: Über die automorphismengruppe eines algebraischen funktionenkörpers von primzahlcharakteristik. Arch. Math. **24**(1), 527–544 (1973).
8. Henning S.: Algebraic Function Fields and Codes, vol. 254. Springer, Berlin (2009).
9. Hirschfeld James W.P., Gábor K., Fernando T.: Algebraic Curves over a Finite Field. Princeton Series in Applied Mathematics. Princeton University Press, Princeton (2008).
10. Jonathan K., Luca T.: On the efficiency of local decoding procedures for error-correcting codes. In: Proceedings of the 32nd Symposium on Theory of Computing, STOC 2000, pp. 80–86 (2000).
11. Kathryn H., Beth M., Matthews Gretchen L.: Locally recoverable codes with availability t≥2 from fiber products of curves. Adv. Math. Commun. **12**(2), 317 (2018).
12. Luna F.-F.S., Venkatesan G., Mary W.: Locality via partially lifted codes. *CoRR*, arXiv:1704.08627 (2017).

13. Nikita P., Ilya V.: Trivariate lifted codes with disjoint repair groups. In: 2019 XVI International Symposium on Problems of Redundancy in Information and Control Systems (REDUNDANCY), pp. 64–68. IEEE (2019).
14. Ray L., Mary W.: Improved list-decodability of random linear binary codes. In: Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik (2018).
15. Ronitt R., Madhu S.: Robust characterizations of polynomials with applications to program testing. SIAM J. Comput. **25**(2), 252–271 (1996).
16. Stichtenoth H.: A note on Hermitian codes over $GF(q^2)$. IEEE Trans. Inf. Theory **34**(5), 1345–1348 (1988).
17. Tiersma H.J.: Remarks on codes from Hermitian curves. IEEE Trans. Inf. Theor. **33**(4), 605–609 (1987).
18. Vitaly S.: Batch and PIR codes and their connections to locally repairable codes. Network Coding and Subspace Designs, pp. 427–442. Springer, Berlin (2018).
19. Woodruff D.P.: A quadratic lower bound for three-query linear locally decodable codes over any field, pp. 766–779. Springer, Heidelberg (2010).
20. Wu L.: Revisiting the multiplicity codes: a new class of high-rate locally correctable codes. In: 2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 509–513. IEEE (2015).
21. Yang K., Vijay K.P.: On the true minimum distance of Hermitian codes. Coding Theory and Algebraic Geometry, pp. 99–107. Springer, Berlin (1992).
22. Yekhanin S.: Locally decodable codes. Found. Trends Theoret. Comput. Sci. **6**(3), 139–255 (2012).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.