Quadratic-Curve-Lifted Reed-Solomon Codes

Hedongliang Liu[1][0000−0001−7512−0654], Lukas Holzbaur[1][0000−0002−8048−3051], Nikita Polyanskii[2][0000−0003−2626−8139], Sven Puchinger[3][0000−0002−7474−2678], and Antonia Wachter-Zeh[1][0000−0002−5174−1947] ⋆

[1] Technical University of Munich, Germany
[2] IOTA Foundation, Germany
[3] HENSOLDT Sensors GmbH, Germany

Abstract. Lifted codes are a class of evaluation codes attracting more attention due to good locality and intermediate availability. In this work we introduce and study *quadratic-curve-lifted Reed-Solomon (QC-LRS) codes*, which is a class of bivariate evaluation codes and the codeword symbols whose coordinates are on a quadratic curve form a codeword of a Reed-Solomon code. We first develop a necessary and sufficient condition on the monomials which form a basis of the code. Based on the condition, we give upper and lower bounds on the dimension and show that the asymptotic rate of a QC-LRS code over $\mathbb{F}_q$ with local redundancy r is $1 - \Theta(q/r)^{-0.2284}$. Moreover, we provide analytical results on the minimum distance of this class of codes and compare QC-LRS codes with lifted Reed-Solomon codes by simulations in terms of the local recovery capability against erasures. For short lengths, QC-LRS codes have better performance in local recovery for erasures than LRS codes of the same dimension.

Keywords: Lifted Codes · Reed-Solomon Codes · Quadratic Curves · Locality · Dimension.

1 Introduction

Lifted codes were introduced by Guo, Kopparty and Sudan [4] as evaluation codes obtained from multivariate polynomials over finite fields. Informally, the key property of these codes is that the restriction to any affine subspace of fixed dimension of the evaluation space is a codeword of a fixed base code. A setting of particular interest, referred to as lifted Reed-Solomon (LRS) codes, is given by lifted codes where each 1-dimensional affine subspace is a codeword of an RS code. This can be viewed as a generalization of the well-known Reed-Muller codes. A surprising advantage of LRS codes is that they achieve much larger asymptotic code rate as the field size grows compared to Reed-Muller (RM) code. The dimension of LRS codes is analyzed via the number of *good monomials*, i.e., the number of multi-variate monomials that result in a codeword of the base code

⋆ The work of H. Liu has been supported by a German Israeli Project Cooperation (DIP) grant under grant no. PE2398/1-1 and KR3517/9-1. The work of L. Holzbaur, N. Polyanskii, and A. Wachter-Zeh was supported by the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG) under Grant No. WA3907/1-1.

when evaluated on any fixed line. The linear span of these good monomials is shown to generate the entire lifted code. The study of these codes was continued in [14,6], where tight asymptotic bounds on the rate were derived.

The seminal paper [4] gave rise to a number of related concepts and code constructions. The works [10,16,7] consider lifting of *multiplicity codes* [8], another class of codes with good locality properties. *Degree-lifted* codes were introduced in [2], where each codeword polynomial is constructed as the product of the uni-variate polynomials in the base code with an additional constraint on the total degree. A class of lifted codes based on code automorphisms was introduced in [3]. Codes constructed from all bivariate polynomials, evaluated on the Hermitian curve, such that the restriction to any line agrees with some low-degree univariate polynomial on the points of the Hermitian curve intersected with that line were analyzed in [12] and named *Hermitian-lifted codes*. A variant of lifted codes that utilizes the trace operation to obtain binary codes with good locality properties was introduced in [5] and coined *wedge-lifted codes*. Thanks to the comments from an anonymous reviewer, we noticed that the recent work [9] gave a more general definition of lifted codes with curves, which is called *weighted lifted codes*. The QC-LRS code (Definition 1) studied in this work is coincidentally identical to [9, Def. IV.1] with $\eta = 2$.

1.1 Main Contribution and Organization

All works mentioned above consider the restriction to linear subspaces or code automorphisms. Our work provides a class of evaluation codes whose local recovery sets correspond to a set of quadratic curves. The advantage of this construction is that there is a much larger number of recovery sets for each codeword symbol, however, these recovery sets do no longer (necessarily) intersect in only one position. This work is devoted to the analysis of the rate and distance of these codes, as well as their local recovery capability compared to LRS/RM codes.

We first investigate the dimension of QC-LRS codes. Since QC-LRS codes are evaluation codes, we analyze the dimension by first deriving the necessary and sufficient condition on the good monomials, where we take similar approaches as in [5], and then by showing that these good monomials form a basis of the code as in [10]. By quantifying the bad monomials following the approach for LRS codes from [6], we derive upper and lower bounds on the dimension of QC-LRS codes over $\mathbb{F}_q$ with q being a power of two. The asymptotic rate of QC-LRS codes over $\mathbb{F}_q$ with local redundancy r is shown to be $1 - \Theta((q/r)^{-0.2284})$. The approach in this paper gives a more precise estimation of the dimension than that in [9], which studied a more general definition of lifted codes with curves of arbitrary degree. To study the advantage of more local groups given by the new notion of QC-LRS codes than LRS codes, we compare between LRS codes and QC-LRS codes the failure probability of locally recovering codeword symbols from erasures. The simulation results show that for the blocklength 64 and under the same code dimension, QC-LRS codes have similar or better performance than LRS codes.

The organization of this paper is as follows: Section 2 introduces the notations used throughout the paper and some basics, which are required in the proofs of the main results. In Section 3 we formally define the QC-LRS codes and present results on the dimension and distance. Due to the page limit, we omit some proofs and we refer to the full version of this paper [11] for an extensive justification. Section 4 presents the comparison on the failure probability of local recovery from erasures by QC-LRS and LRS codes.

2 Preliminaries

Denote the set of integers $\{a,\ldots,b\}$ by $[a,b]$ and by $[b]$ if $a=1$. A finite field of size q is denoted by $\mathbb{F}_q$. The integer ring of size q is denoted by $\mathbb{Z}_q$. Let $\deg:\mathbb{F}_q[x]\to\mathbb{N}$ be the degree function of univariate polynomials. For any $f=\sum_{i=0}^{q-1}f_ix^i$, $\deg(f)=\max\{i|f_i\neq 0\}$. For non-negative integers $a,b\in\mathbb{N}$ with *binary representations* $a=(a_0,\ldots,a_{\ell-1})_2$, $b=(b_0,\ldots,b_{\ell-1})_2$, we say that a *lies in the 2-shadow of* b, denoted by $a\leqslant_2 b$, if $a_i\leqslant b_i,\ \forall i\in[0,\ell-1]$. The bit $a_{\ell-1}$ is the most significant bit in the binary representation of a. For a bi-variate function $f:\mathbb{F}_q^2\to\mathbb{F}_q$ and a set $D\subset\mathbb{F}_q^2$, let $f|_D$ denote the restriction of f to the domain D. If D is the set of points corresponding to the roots in $\mathbb{F}_q^2$ of a bi-variate function $\phi:\mathbb{F}_q^2\to\mathbb{F}_q$, i.e., $D=\{(x,y)\in\mathbb{F}_q^2\mid\phi(x,y)=0\}$, we denote by $f|_\phi$ the restriction of f to the *curve* ϕ. A bivariate function $\phi:\mathbb{F}_q^2\to\mathbb{F}_q$ is a *quadratic function* or *quadratic curve* if it is in the form $\phi(x,y)=y+\alpha x^2+\beta x+\gamma$, where $\alpha,\beta,\gamma\in\mathbb{F}_q$.

Define an operation $(\bmod^*\ q)$ that takes a non-negative integer and maps it to an element in $[0,q-1]$ as follows

$$a \ (\bmod^*\ q) := \begin{cases} a, & \text{if } a\leqslant q-1 \\ q-1, & \text{if } a \ (\bmod\ q-1)=0, a\neq 0 \\ a \ (\bmod\ q-1), & \text{else} \end{cases}$$

It can be readily seen that if $a\ (\bmod^*\ q)=b$, then $x^a=x^b\ (\bmod\ x^q-x)$ in $\mathbb{F}_q[x]$.

Lemma 1 (Lucas' Theorem [13]). *Let p be a prime and $a,b\in\mathbb{N}$ be written in p-ary representations $a=(a_0,\ldots,a_{\ell-1})_p$, $b=(b_0,\ldots,b_{\ell-1})_p$. Then*

$$\binom{a}{b}=\prod_{i=1}^{\ell}\binom{a_i}{b_i} \mod p\ .$$

If $p=2$, then $\binom{a}{b}=1$ if and only if $b\leqslant_2 a$.

Lemma 2 (Combinatorial Nullstellensatz [1, Theorem 1.2]). *Let $\mathbb{F}$ be an arbitrary field, and let $f(x_1,\ldots,x_m)$ be a multivariate polynomial in $\mathbb{F}[x_1,\ldots,x_m]$ of degree $\deg(f)=\sum_{i=1}^m t_i$, where each t_i is a non-negative integer, and suppose the coefficient of $\prod_{i=1}^m x_i^{t_i}$ in f is nonzero. Then, if $S_1,\ldots,S_m$ are subsets of $\mathbb{F}$ with $|S_i|>t_i$, there are $s_1\in S_1,\ldots,s_m\in S_m$ so that*

$$f(s_1,\ldots,s_m)\neq 0.$$

3 Quadratic-Curve-Lifted Reed-Solomon Codes

In this section, we first give a general definition of curve-lifted Reed-Solomon codes and present our results on a specific class of codes, the QC-LRS codes, with restriction to quadratic curves.

Definition 1 (Curve-Lifted Reed-Solomon Codes). *Let q be a power of 2 and Φ be a set of bi-variate functions. A curve-lifted Reed-Solomon code is defined by*

$$\mathcal{C}_q(\Phi, d) := \{f : \mathbb{F}_q^2 \to \mathbb{F}_q \mid \deg(f|_\phi) < d, \forall \phi \in \Phi\} \ .$$

In order to investigate the dimension of curve-lifted RS codes, we introduce the *good monomials*[4], which is a tool also used in studying LRS codes in [4,6].

Definition 2 ($(\Phi, d)^*$-good monomial). *Given a set Φ of bi-variate functions, a monomial $m(x, y) = x^a y^b$ is* $(\Phi, d)^*$-good *if* $\deg(m|_\phi) < d, \forall \phi \in \Phi$. *The monomial is* $(\Phi, d)^*$-bad *otherwise.*

In the following let Φ be the set of all quadratic functions[5] over $\mathbb{F}_q$, i.e.,

$$\Phi := \{\phi(x, y) = y + \alpha x^2 + \beta x + \gamma, \forall \alpha, \beta, \gamma \in \mathbb{F}_q\} \tag{1}$$

and we present the results on QC-LRS codes.

The following Lemma 3 gives a necessary and sufficient condition such that a monomial $m(x, y) = x^a y^b$ is $(\Phi, d)^*$-good.

Lemma 3. *Let q be a power of 2, Φ be the set of all quadratic functions over $\mathbb{F}_q$ and $a, b < q$ be integers. A monomial $m(x, y) = x^a y^b$ is $(\Phi, d)^*$-good if and only if*

$$2i + j + a \ (\mathrm{mod}^* \ q) < d, \ \forall i \leqslant_2 b, \ j \leqslant_2 b - i \ . \tag{2}$$

3.1 Dimension of Quadratic-Curve-Lifted RS Codes

The first important result is that the dimension of the code is exactly the number of good monomials, which we present in Theorem 1. In order to show that, we first discuss in the following lemma a special case that will be excluded in the proof of Theorem 1. Due to space limitations, we leave out the proof of the lemma here and refer to the full version of this paper [11].

Lemma 4. *Consider two monomials $m_1(x, y) = x^{q-1} y^b$ and $m_2(x, y) = y^b$ with $0 \leqslant b \leqslant q - 1$ and a polynomial $P(x, y)$ containing m_1 and m_2, i.e.,*

$$P(x, y) = (\xi_1 x^{q-1} y^b + \xi_2 y^b) + P'(x, y)$$

where $\xi_1, \xi_2 \neq 0$ and $P'(x, y)$ does not contain m_1 or m_2. Then, P is $(\Phi, d)^*$-bad for any $d \leqslant q - 1$.

Theorem 1 (Dimension is the number of good monomials). *Let $d \leqslant q - 1$ and Φ be the set of all quadratic functions. The QC-LRS code $\mathcal{C}_q(\Phi, d)$ has dimension equal to the number of $(\Phi, d)^*$-good monomials over $\mathbb{F}_q$.*

---

[4] This is a short notation to easily address these monomials later. There is no bias on the performance of the monomials.

[5] This set is a subset of quadratic curves, which are often referred as *conics* in geometry. This set is also identical to the set of *affine η-lines* defined in [9] with $\eta = 2$.

Proof. Assume a polynomial P containing $(\Phi, d)^*$-bad monomials is $(\Phi, d)^*$-good. Let $\mathcal{G}$ and $\mathcal{B}$ be subsets of indices of all $(\Phi, d)^*$-good and -bad monomials, respectively (assuming the monomials are ordered according to some order). We can write P as

$$P = \sum_{c \in \mathcal{G}} \xi_c x^{a_c} y^{b_c} + \sum_{c \in \mathcal{B}} \xi_c x^{a_c} y^{b_c},$$

with $\xi_c \in \mathbb{F}_q \setminus \{0\}$. Restricting P to the quadratic curve $\phi : y = \alpha x^2 + \beta x + \gamma$ is the univariate polynomial

$$\begin{aligned} P|_\phi &= \sum_{c \in \mathcal{G} \cup \mathcal{B}} \xi_c x^{a_c} (\alpha x^2 + \beta x + \gamma)^{b_c} \\ &= \sum_{c \in \mathcal{G} \cup \mathcal{B}} \xi_c \sum_{i=0}^{b_c} \sum_{j=0}^{b_c - i} \binom{b_c}{i} \binom{b_c - i}{j} \alpha^i \cdot \beta^j \cdot \gamma^{b_c - i - j} \cdot x^{2i + j + a_c}. \end{aligned}$$

Let $P|_\phi^* = P|_\phi \bmod (x^q - x)$. Denote by $[x^s]P|_\phi^*$ the coefficient of x^s in $P|_\phi^*$. By Lucas' Theorem (see Lemma 1), we have

$$[x^s]P|_\phi^* = \sum_{c \in \mathcal{G} \cup \mathcal{B}} \sum_{\substack{i \leqslant_2 b_c,\ j \leqslant_2 b_c - i \\ 2i + j + a_c \pmod{^*}\ q) = s}} \xi_c \cdot \alpha^i \cdot \beta^j \cdot \gamma^{b_c - i - j}.$$

For $s \geqslant d$, the $(\Phi, d)^*$-good monomials do not contribute to these coefficients (see Definition 2), therefore,

$$[x^s]P|_\phi^* = \sum_{c \in \mathcal{B}} \sum_{\substack{i \leqslant_2 b_c, j \leqslant_2 b_c - i \\ 2i + j + a_c \pmod{^*}\ q) = s}} \xi_c \cdot \alpha^i \cdot \beta^j \cdot \gamma^{b_c - i - j} \quad \text{for } s \geqslant d. \tag{3}$$

We view $[x^s]P|_\phi^*$ as a trivariate polynomial in α, β, γ. Note that P is $(\Phi, d)^*$-good only if

$$[x^s]P|_\phi^* \ (\alpha, \beta, \gamma) = 0\ , \quad \forall \alpha, \beta, \gamma \in \mathbb{F}_q, \forall s \geqslant d\ . \tag{4}$$

Now consider two bad monomials $x^{a_c} y^{b_c}$ and $x^{a_d} y^{b_d}$ with $c, d \in \mathcal{B}$. Then the corresponding terms in (3) contributed by them can be added up only if $\alpha^{i_c} \beta^{j_c} \gamma^{b_c - i_c - j_c} = \alpha^{i_d} \beta^{j_d} \gamma^{b_d - i_d - j_d}$, which is true if and only if

$$\Longleftrightarrow \begin{cases} i_c = i_d \\ j_c = j_d \\ b_c - i_c - j_c = b_d - i_d - j_d \\ 2i_c + j_c + a_c \pmod{^*}\ q) = 2i_d + j_d + a_d \pmod{^*}\ q) \end{cases}$$

$$\Longrightarrow \begin{cases} b_c = b_d \\ |a_c - a_d| = 0 \text{ or } q - 1\ . \end{cases}$$

For the case $|a_c - a_d| = q - 1$, such polynomials are bad according to Lemma 4. For the case $|a_c - a_d| = 0$, we can conclude that the monomials $\alpha^i \beta^j \gamma^{b_c - i - j}$ are distinct for different pairs of (a_c, b_c). Namely, (3) is in its simplest form[6].

Assume $\mathcal{B}$ is non-empty. Since $\xi_c \neq 0$ for all c, (3) is a non-zero polynomial. By Lemma 2, since the variables $\alpha, \beta, \gamma \in \mathbb{F}_q$ and all exponents $i, j, b_c - i - j < q$, there exists some $\alpha_0, \beta_0, \gamma_0 \in \mathbb{F}_q$, such that $[x^s]P|_\phi^* \neq 0$. This contradicts the assumption that P is $(\Phi, d)^*$-good. This implies that (4) can be fulfilled only if

[6] No similar terms can be further combined.

$[x^s]P|_{\phi}^*$ is a zero polynomial, i.e., $\mathcal{B}$ is empty. Hence, a polynomial P is $(\Phi, d)^*$-good only if it only consists of good monomials. □

3.2 Estimation of the Dimension

In this section we provide an analysis of the dimension of QC-LRS codes $\mathcal{C}_q(\Phi, d = q - r)$, where $q = 2^\ell$ and $r \in [q-1]$. Recall from Lemma 3 that a monomial $m(x, y) = x^a y^b$ is $(\Phi, q-r)^*$-bad if and only if there exist $i \leqslant_2 b$ and $j \leqslant_2 b - i$ such that $2i + j + a \pmod{^* q} \geqslant q - r$. We will first consider a slightly different definition of a bad monomial to simplify our arguments. Then, we derive upper and lower bounds on the number of $(\Phi, q-r)^*$-bad monomials and further establish the results on the rate of QC-LRS codes.

Counting $(\Phi, q-r)$-bad monomials: Let $q = 2^\ell$ and $r \in [q-1]$. We say that a monomial $m(x, y) = x^a y^b$ (or the pair (a, b)) is $(\Phi, q-r)$-bad if and only if there exist $i \leqslant_2 b$ and $j \leqslant_2 b - i$ such that $2i + j + a \pmod q \geqslant q - r$. For an integer $t \geqslant 0$, we define

$$S_t(\ell) = \left\{ (a, b) \in \mathbb{Z}_q^2 \ : \ \begin{array}{l} \exists\, i \leqslant_2 b, j \leqslant_2 b - i, \\ \text{s.t. } 2i + j + a = q - r' + tq, \text{ for some } r' \in [r] \end{array} \right\} \tag{5}$$

For $1 \leqslant r < q$ and $t \geqslant 3$, the set $S_t(\ell)$ is empty as $2i + j + a \leqslant i + b + a \leqslant 2b + a \leqslant 3(q-1) < q - r + tq$. Hence, if $x^a y^b$ is $(\Phi, q-r)$-bad, then $(a, b) \in S_0(\ell) \cup S_1(\ell) \cup S_2(\ell)$.

In what follows, we assume that $1 \leqslant r < q$ and attempt to derive some recursive relations on $S_0(\ell)$, $S_1(\ell)$ and $S_2(\ell)$. We have two observations in Lemma 5 and Lemma 6.

Lemma 5. *Let $q = 2^\ell$ and $r < \frac{q}{2}$, $a = (a_0, \ldots, a_{\ell-1})_2$ and $b = (b_0, \ldots, b_{\ell-1})_2$. Define $a' := (a_0, \ldots, a_{\ell-2})_2$ and $b' := (b_0, \ldots, b_{\ell-2})_2$. If $(a, b) \in S_0(\ell) \cup S_1(\ell) \cup S_2(\ell)$, then $(a', b') \in S_0(\ell-1) \cup S_1(\ell-1) \cup S_2(\ell-1)$.*

Lemma 6. *For $t = 1, 2$, if $(a, b) \in S_t(\ell)$, then $(a, b) \in S_{t-1}(\ell)$.*

It follows from Lemma 6 that $x^a y^b$ is $(\Phi, q-r)$-bad if and only if $(a, b) \in S_0(\ell)$.

Based on the observations in Lemma 6 and Lemma 5, we provide a recursive formula for computing the size of $S_t(\ell)$ for $t = 0, 1, 2$.

Lemma 7. *For $1 \leqslant r < \frac{q}{2}$, it holds that*

$$|S_0(\ell)| = 3|S_0(\ell-1)| + |S_1(\ell-1)|,$$
$$|S_1(\ell)| = |S_0(\ell-1)| + |S_1(\ell-1)| + |S_2(\ell-1)|,$$
$$|S_2(\ell)| = |S_2(\ell-1)|.$$

Lemma 7 yields a recurrence relation for $|S_0(\ell)|$, $|S_1(\ell)|$ and $|S_2(\ell)|$. For a given r, the initial value ℓ_0 should be chosen such that $S_i(\ell_0), i = 0, 1, 2$ is a valid set according to the definition in (5). Denote by $\boldsymbol{s}(\ell) = (|S_0(\ell)|, |S_1(\ell)|, |S_2(\ell)|)^\top$. We then have

$$\boldsymbol{s}(\ell) = \boldsymbol{A}^{\ell-\ell_0} \cdot \boldsymbol{s}(\ell_0), \quad \text{where } \boldsymbol{A} = \begin{pmatrix} 3 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}. \tag{6}$$

The recursion enables us to find the asymptotic behavior of the number of $(\Phi, q-r)$-bad monomials, which is exactly $|S_0(\ell)|$. Note that the order of $|S_j(\ell)|, j = 0, 1, 2$ is controlled by λ_1^ℓ, where $\lambda_1 = 2+\sqrt{2}$ is the largest eigenvalue of $\boldsymbol{A}$ in (6). Hence,

$$|S_0(\ell)| = \Theta((2+\sqrt{2})^\ell). \tag{7}$$

For different r, the exact values of $|S_0(\ell)|$ can be different, since the initial value $|S_0(\ell_0)|$ depends on r. However, the asymptotic behavior is the same for any fixed r.

We provide the exact expressions of $|S_0(\ell)|$ for $r = 1$ and $r = 3$, denoted by $|S_0^{(1)}(\ell)|$ and $|S_0^{(3)}(\ell)|$ respectively, which we will later use to derive upper and lower bound on the number of $(\Phi, q-r)^*$-bad monomials:

$$\begin{aligned}|S_0^{(1)}(\ell)| =& \frac{5\sqrt{2}+7}{2(3\sqrt{2}+4)} \cdot \lambda_1^\ell + \frac{5\sqrt{2}-7}{2(3\sqrt{2}-4)} \cdot \lambda_2^\ell \\ \approx& 0.8536 \cdot \lambda_1^\ell + 0.1464 \cdot \lambda_2^\ell \end{aligned}\tag{8}$$

$$\begin{aligned}|S_0^{(3)}(\ell)| =& \frac{65\sqrt{2}+92}{4(12\sqrt{2}+17)} \cdot \lambda_1^\ell + \frac{65\sqrt{2}-92}{4(12\sqrt{2}-17)} \cdot \lambda_2^\ell - \lambda_3^\ell \\ \approx& 1.3536 \cdot \lambda_1^\ell + 0.6465 \cdot \lambda_2^\ell - 1 \end{aligned}\tag{9}$$

where $\lambda_1 = 2+\sqrt{2}, \lambda_2 = 2-\sqrt{2}, \lambda_3 = 1$ are the three distinct eigenvalues of the matrix $\boldsymbol{A}$.

Counting $(\boldsymbol{\Phi}, \boldsymbol{q-r})^*$-bad monomials: For $q = 2^\ell$ and $1 \leqslant r < q$, we define the following set

$$S^*(\ell) := \left\{ (a,b) \in \mathbb{Z}_q^2 \ : \begin{array}{r} \exists\ i \leqslant_2 b, j \leqslant_2 b-i,\ \text{s.t. } 2i+j+a = q-r'+t(q-1), \\ \text{for some } r' \in [r], t \geqslant 0 \end{array} \right\}.$$

It is clear that $(a,b) \in S^*(\ell)$ if and only if $x^a y^b$ is $(\Phi, q-r)^*$-bad.

We first relate the value $|S^*(\ell)|$ to $|S_0(\ell)|$ in Lemma 8 and Lemma 9.

Lemma 8. *Let $\ell \geqslant 2, q = 2^\ell$, $1 \leqslant r \leqslant \frac{q}{4}$, $s = \lceil \log_2(r) \rceil$ and $q' = 2^{\ell-s}$. Denote by $S_0^{(3)}(\ell-s)$ the set of (a,b) such that $x^a y^b$ is $(\Phi, q'-3)$-bad. Then*

$$|S^*(\ell)| < 4r^2 \cdot |S_0^{(3)}(\ell-s)|.$$

If r is a power of 2, then

$$|S^*(\ell)| \leqslant r^2 \cdot |S_0^{(3)}(\ell-s)|.$$

Lemma 9. *Let $\ell \geqslant 1, q = 2^\ell$, $1 \leqslant r \leqslant \frac{q}{2}$, $s = \lfloor \log_2 r \rfloor$ and $q' = 2^{\ell-s}$. Denote by $S_0^{(1)}(\ell-s)$ the set of (a,b) such that $x^a y^b$ is $(\Phi, q'-1)$-bad. Then*

$$|S^*(\ell)| > \frac{r^2}{4} \cdot |S_0^{(1)}(\ell-s)|\ .$$

If r is a power of 2, then

$$|S^*(\ell)| \geqslant r^2 \cdot |S_0^{(1)}(\ell-s)|\ .$$

In the following theorem we provide the exact expressions of upper and lower bounds on $|S^*(\ell)|)$, using the exact expression of $|S_0(\ell)|$ in (8) and (9).

Theorem 2. *Let $\ell \geqslant 2, q = 2^\ell, 1 \leqslant r \leqslant \frac{q}{4}$ and $s = \log_2 r$, the number of $(\Phi, q-r)^*$-bad monomials is*

$$\frac{0.8536 \cdot \lambda_1^{\ell-\lfloor s \rfloor} + 0.1464 \cdot \lambda_2^{\ell-\lfloor s \rfloor}}{4} < \frac{|S^*(\ell)|}{r^2} < 4(1.3536 \cdot \lambda_1^{\ell-\lceil s \rceil} + 0.6465 \cdot \lambda_2^{\ell-\lceil s \rceil} - 1) ,$$

where $\lambda_1 = 2 + \sqrt{2}$ and $\lambda_2 = 2 - \sqrt{2}$.

If r is a power of 2, we obtain

$$0.8536 \cdot \lambda_1^{\ell-s} + 0.1464 \cdot \lambda_2^{\ell-s} \leqslant \frac{|S^*(\ell)|}{r^2} \leqslant 1.3536 \cdot \lambda_1^{\ell-s} + 0.6465 \cdot \lambda_2^{\ell-s} - 1 .$$

We can then derive an asymptotic behavior of the rate of QC-LRS codes in Corollary 1.

Corollary 1. *Let $\mu = \log_2(2+\sqrt{2})$. For $q \to \infty$ and $1 \leqslant r \leqslant \frac{q}{4}$, the number of $(\Phi, q-r)^*$-bad monomials is*

$$|S^*(\ell)| = \Theta(r^{2-\mu} q^\mu) .$$

Further, the QC-LRS code $\mathcal{C}_q(\Phi, q-r)$ has rate

$$R = 1 - \Theta\left((q/r)^{\mu-2}\right) = 1 - \Theta\left((q/r)^{-0.2284}\right) .$$

For an illustration, we plot in Fig. 1 the dimension of the code $\mathcal{C}_q(\Phi, q-r)$ with $q = 2^5$, which is done by computer-search according to the necessary and sufficient condition in Lemma 3, and the corresponding lower and upper bounds for $r \in [1, q/4]$ based on the bounds on $|S^*(\ell)|$ in Theorem 2.

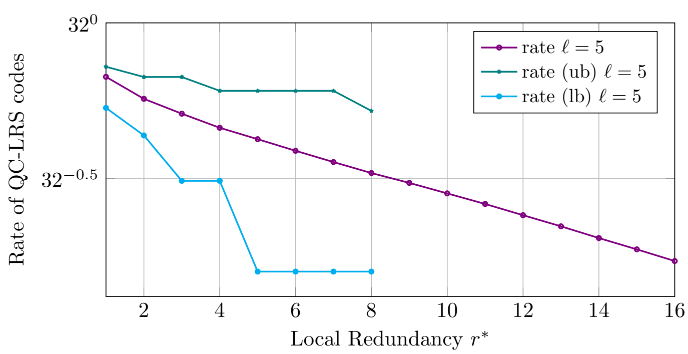

Fig. 1: The dimension of QC-LRS code $\mathcal{C}_q(\Phi, q-r)$ with $q = 2^5$ along with the corresponding upper bound (ub) and lower bound (lb) for $r \in [1, q/4]$ calculated by $1 - |S^*(\ell)|/q^2$. The lower and upper bound on $|S^*(\ell)|$ are given in Theorem 2.

Remark 1. Recall that the rate of bivariate lifted Reed-Solomon (LRS) codes is $R = 1 - \Theta((q/r)^{\log_2 3 - 2} = 1 - \Theta((q/r)^{-0.4150})$ [6]. We compare the performance of our codes with LRS codes in terms of local recovery in an erasure channel in Section 4.

3.3 Distance of Quadratic-Curve-Lifted RS Codes

We provide the upper and lower bounds on the distance of the QC-LRS codes $\mathcal{C}_q(\Phi, q-r)$ in the following theorem.

Theorem 3 (Bounds on the Minimum Distance). *Let q be a power of 2 and Φ be the set of all quadratic functions. The QC-LRS code $\mathcal{C}_q(\Phi, q-r)$ has minimum distance*

$$qr + 1 \leqslant \operatorname{dist}(\mathcal{C}_q(\Phi, q-r)) \leqslant qr + q \ .$$

Proof. The upper bound is proven by counting the number of zeros in the codeword $f(x, y) = \prod_{\alpha \in \mathcal{A}}(x - \alpha)$, where $\mathcal{A}$ is a subset of $\mathbb{F}_q$ with $|\mathcal{A}| = q - r - 1$. The lower bound is proven by considering the minimum number of non-zero positions in all disjoint local groups (e.g., all lines) of a non-zero symbol in a codeword. For a detailed proof we refer to the full version of this paper [11].Note that the bounds are derived in a similar method as for LRS codes in [4, Theorem 5.1]. □

4 Local Recovery Capability from Erasures

For a code with locality [15], the local groups of a codeword symbol are defined as the sets of indices where the symbol can be recovered by accessing only the symbols in one of the sets. Given a QC-LRS code over $\mathbb{F}_q$, the number of local recovery sets of any codeword symbol is the number of quadratic curves over $\mathbb{F}_q$ passing through a certain point, which is q^2. For an LRS codes, the number of local recovery sets is $q + 1$. Consider an erasure channel with erasure probability τ. With respect to the local recovery, we are interested in correcting a certain erasure within a local recovery set and how large the failure probabilities of LRS/QC-LRS codes is. The failure probability is exactly the probability that there are at least r other erasures in each local recovery set of the erased symbol to be recovered. For LRS codes, since all the local recovery sets are disjoint, the failure probability is exactly $\left(\sum_{i=r}^{q-1} \binom{q-1}{i} \tau^i (1-\tau)^{q-1-i}\right)^{q+1}$. For QC-LRS codes, since the local recovery sets may intersect with each other, an analysis for the closed form of the failure probability is still an open problem. In order to compare the performance of these two codes, we run simulations with both codes of length $n = 64$, dimension $k = 10$ and $k = 6$, respectively. The simulation results are presented in Fig. 2. We can see that for both $\dim = 10$ and $\dim = 6$, the failure probability of local recovery with QC-LRS is smaller than or similar to that with LRS codes for $\tau \leqslant 0.7$. Therefore, for this length, QC-LRS codes perform better than LRS for local recovery.

References

1. Alon, N.: Combinatorial Nullstellensatz. Combinatorics, Probability and Computing **8**(1-2), 7–29 (1999)
2. Ben-Sasson, E., Gabizon, A., Kaplan, Y., Kopparty, S., Saraf, S.: A new family of locally correctable codes based on degree-lifted algebraic geometry codes. p. 833–842. STOC '13, Assoc. Comput. Machinery (2013)
3. Guo, A.: High-rate locally correctable codes via lifting. IEEE Trans. Inf. Theory **62**(12), 6672–6682 (2016)
4. Guo, A., Kopparty, S., Sudan, M.: New affine-invariant codes from lifting. In: Proc. 4th Conf. Innov. Theor. Comput. Sc. pp. 529–540 (2013)
5. Hastings, J., Kanne, A., Li, R., Wootters, M.: Wedge-lifted codes. In: Proc. 2021 IEEE Int. Symp. Inf. Theory (ISIT). pp. 2990–2995

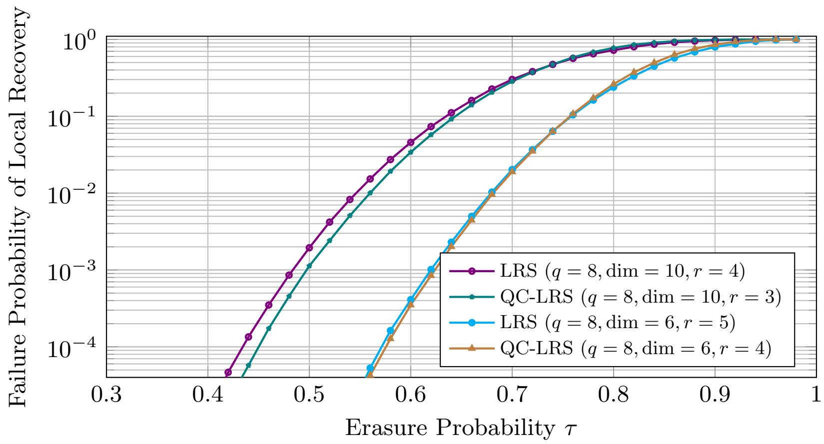

Fig. 2: Local recovery performance of LRS/RM and QC-LRS ($\mathcal{C}_q(\Phi, d = q - r)$) codes of length $n = q^2 = 64$ dimension $k = 10$ (rate $= k/n = 0.15625$) and dimension $k = 6$ (rate $= k/n = 0.09375$). Note that the LRS codes with the parameters here are RM codes.

6. Holzbaur, L., Polyanskaya, R., Polyanskii, N., Vorobyev, I.: Lifted Reed-Solomon codes with application to batch codes. In: Proc. 2020 IEEE Int. Symp. Inf. Theory (ISIT). pp. 634–639
7. Holzbaur, L., Polyanskaya, R., Polyanskii, N., Vorobyev, I., Yaakobi, E.: On lifted multiplicity codes. In: Proc. 2020 IEEE Inf. Theory Workshop (ITW). pp. 1–5
8. Kopparty, S., Saraf, S., Yekhanin, S.: High-rate codes with sublinear-time decoding. J. ACM **61**(5), 1–20 (2014)
9. Lavauzelle, J., Nardi, J.: Weighted lifted codes: Local correctabilities and application to robust private information retrieval. IEEE Trans. Inf. Theory **67**(1), 111–123 (2020)
10. Li, R., Wootters, M.: Lifted multiplicity codes and the disjoint repair property. Leibniz Int. Proc. Inform. (2019)
11. Liu, H., Holzbaur, L., Polyanskii, N., Puchinger, S., Antonia, W.Z.: Quadratic-curve-lifted Reed-Solomon codes (2021), https://arxiv.org/abs/2109.14478
12. López, H.H., Malmskog, B., Matthews, G.L., Piñero-González, F., Wootters, M.: Hermitian-lifted codes. Des. Codes Cryptogr. **89**(3), 497–515 (2021)
13. Lucas, E.: Théorie des fonctions numériques simplement périodiques. Amer. J. Math. **1**(2), 184–196 (1878)
14. Polyanskii, N., Vorobyev, I.: Trivariate lifted codes with disjoint repair groups. In: 2019 XVI Int. Symp. "Problems of Redundancy in Information and Control Systems" (REDUNDANCY). pp. 64–68. IEEE
15. Tamo, I., Barg, A.: A family of optimal locally recoverable codes. IEEE Trans. Inf. Theory **60**(8), 4661–4676 (2014)
16. Wu, L.: Revisiting the multiplicity codes: A new class of high-rate locally correctable codes. In: 2015 53rd Annu. Allerton Conf. on Commun., Control, and Comput. pp. 509–513. IEEE