Construction of Optimal Locally Repairable Codes via Automorphism Groups of Rational Function Fields

Lingfei Jin, Liming Ma, and Chaoping Xing

Abstract—Locally repairable codes, or locally recoverable codes (LRC for short), are designed for applications in distributed and cloud storage systems. Similar to classical block codes, there is an important bound called the Singleton-type bound for locally repairable codes. In this paper, an optimal locally repairable code refers to a block code achieving this Singleton-type bound. Like classical MDS codes, optimal locally repairable codes carry some very nice combinatorial structures. Since the introduction of the Singleton-type bound for locally repairable codes, people have put tremendous effort into construction of optimal locally repairable codes. There are a few constructions of optimal locally repairable codes in the literature. Most of these constructions are realized via either combinatorial or algebraic structures. In this paper, we apply automorphism group of the rational function field to construct optimal locally repairable codes by considering the group action on projective lines over finite fields. Due to various subgroups of the projective general linear group, we are able to construct optimal locally repairable codes with flexible locality as well as smaller alphabet size comparable to the code length. In particular, we produce new families of $q$-ary locally repairable codes, including codes of length $q+1$ via cyclic groups.

Index Terms—Automorphism groups, locally repairable codes, Riemann-Roch spaces, rational function fields.

I. INTRODUCTION

Due to recent applications to distributed and cloud storage systems, a new class of block codes, i.e., locally repairable codes have been investigated by many researchers [2], [3], [6]–[8], [10], [11], [15], [16], [18], [20], [21]. A locally repairable code is just a block code with an additional property called locality. As most of classical block codes do not carry good locality, people have to investigate various constructions of block codes with good locality.

Manuscript received July 4, 2018; revised April 14, 2019; accepted August 30, 2019. Date of publication October 11, 2019; date of current version December 23, 2019. L. Jin was supported in part by the National Natural Science Foundation of China under Grant 11871154 and in part by the Chenguang Program supported by Shanghai Education Development Foundation and Shanghai Municipal Education Commission. L. Ma was supported in part by the NSFC under Grant 11501493, in part by the Lvyang and Jinfeng Program of Yangzhou City, and in part by the China Scholarship Council.

L. Jin is with the Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai 200433, China (e-mail: ljjin@fudan.edu.cn).
L. Ma is with the School of Mathematical Sciences, Yangzhou University, Yangzhou 225002, China (e-mail: limma@yzu.edu.cn).
C. Xing is with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China, and also with the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371 (e-mail: xingcp@sjtu.edu.cn). Communicated by P. Beelen, Associate Editor for Coding Theory.

Block codes with good locality were initially studied in [8], [10], although [10] considered a slightly different definition of locality, under which a code is said to have information locality. Codes with information locality property were also studied in [6], [7]. For a locally repairable code $C$ of length $n$ with $k$ information symbols and locality $r$ (see the definition of locally repairable codes in Section II-A), it was proved in [7] that the minimum distance $d(C)$ of $C$ is upper bounded by

$$d(C) \leq n - k - \left\lfloor \frac{k}{r} \right\rfloor + 2. \quad (1)$$

The bound (1) is called the Singleton-type bound for locally repairable codes and was proved by extending the arguments in the proof of the classical Singleton bound on codes. We refer an optimal locally repairable code to a block code achieving the Singleton-type bound (1).

A. Known Results

Apparently, construction of optimal locally repairable codes, i.e., block codes achieving the bound (1) is of both theoretical interest and practical importance. There are a few constructions available in the literature and hence a few classes of optimal locally repairable codes are known. A class of codes constructed earlier and known as pyramid codes [10] were shown to be optimal locally repairable codes. In [18], Silberstein et al. proposed a two-level construction based on the Gabidulin codes combined with a single parity-check $(r + 1, r)$ code. Another construction in [21] used two layers of MDS codes, a Reed-Solomon code and a special $(r + 1, r)$ MDS code. A common shortcoming of these constructions relates to the size of the code alphabet which in all the papers is an exponential function of the code length, complicating the implementation. There was an earlier construction of optimal locally repairable codes given in [16] with alphabet size comparable to code length. However, the construction in [16] only produced a specific value of the length $n$, i.e., $n = \left\lfloor \frac{k}{r} \right\rfloor (r + 1)$. Thus, the rate of the code is very close to 1.

A recent breakthrough construction was given in [20]. This construction naturally generalizes the Reed-Solomon construction which relies on the alphabet of cardinality comparable to the code length $n$. The idea behind the construction is very nice. The only shortcoming of this construction is the restriction on locality $r$. Namely, $r + 1$ must be a divisor of either $q - 1$ or $q$, or $r + 1$ is equal to some special divisors of $q(q - 1)$. Several isolated $q$-ary optimal locally repairable
codes with length around $q^2$ were constructed from algebraic surfaces in [1].

There are also some existence results given in [16] and [20] with less restriction on locality $r$. But both results require large alphabet size which is an exponential function of the code length.

B. Our Results and Comparison

In this paper, we present a non-trivial generalization of optimal locally repairable codes given in [20] by employing automorphism group of the rational function field. This allows flexibility of locality as well as smaller alphabet of cardinality comparable to the code length $n$. More precisely, as long as there is a subgroup of size $r+1$ in the projective general linear group $\text{PGL}_2(q)$ (see the definition of $\text{PGL}_2(q)$ in Section II-C) with $(r+1)n$ and $n \leq q+1$, we can construct an optimal locally repairable code of length $n$ and locality $r$. Thus, to construct optimal locally repairable codes, we need to find all subgroups of $\text{PGL}_2(q)$. Fortunately, subgroups of $\text{PGL}_2(q)$ have been completely determined in the literature. Thus, we are able to obtain $q$-ary optimal locally repairable codes of length $n$ and locality $r$ as long as there is a subgroup of size $r+1$ in the projective general linear group $\text{PGL}_2(q)$ together with the conditions $(r+1)n$ and $n \leq q+1$.

However, it is unnecessary to write down all subgroups and provide the corresponding constructions of optimal locally repairable codes. Instead, we present a general construction for arbitrary subgroups of $\text{PGL}_2(q)$ in Section III. We then present explicit constructions of optimal locally repairable codes from subgroups of the affine linear group $\text{AGL}_2(q)$ (see definition of $\text{AGL}_2(q)$ in Section II-B). It turns out that the construction given by Tamo and Barg in [20] can be realized by subgroups of the affine linear group $\text{AGL}_2(q)$ under our framework.

In addition, we also present an explicit construction from subgroups of size that divides $q+1$. This construction produces optimal locally repairable codes of length $q+1$ that were not known before. Then in the last section, we give optimal locally repairable codes from subgroups of a dihedral group that can be viewed as a subgroup of $\text{PGL}_2(q)$.

C. Organization of the Paper

In Section II, we introduce some backgrounds for this paper such as the definition of locally repairable codes, the rational function field and its automorphism group, the projective general linear group and its subgroups, Hilbert’s ramification theory, and algebraic geometry codes. Section III devotes to a general construction of optimal locally repairable codes from arbitrary subgroups of $\text{PGL}_2(q)$. In Section IV, we present an explicit construction of optimal locally repairable codes from subgroups of the affine linear group $\text{AGL}_2(q)$. In Sections V and VI, we give explicit constructions of optimal locally repairable codes from subgroups of a cyclic group of order $q+1$ and dihedral groups, respectively. In the last section, we conclude the paper by summarizing our main results of this paper.

II. Preliminaries

In this section, we present some preliminaries on locally repairable codes, the rational function field and its automorphism group, the subgroups of the projective general linear group, Hilbert’s ramification theory, and algebraic geometry codes.

A. Locally Repairable Codes

Informally speaking, a block code is said with locality $r$ if every coordinate of a given codeword can be recovered by accessing at most $r$ other coordinates of this codeword. The formal definition of a locally repairable code with locality $r$ is given as follows.

**Definition 1.** Let $C \subseteq \mathbb{F}_q^n$ be a $q$-ary block code of length $n$. For each $\alpha \in \mathbb{F}_q$ and $i \in \{1, 2, \cdots, n\}$, define $C(\alpha, i) := \{c = (c_1, \ldots, c_n) \in C \mid c_i = \alpha\}$. For a subset $I \subseteq \{1, 2, \cdots, n\} \setminus \{i\}$, we denote by $C_I(\alpha, i) \cap C_I(\beta, i)$ the projection of $C(\alpha, i)$ on $I$. Then $C$ is called a locally repairable code with locality $r$ if, for every $i \in \{1, 2, \cdots, n\}$, there exists a subset $I_i \subseteq \{1, 2, \cdots, n\} \setminus \{i\}$ with $|I_i| \leq r$ such that $C_{I_i}(\alpha, i) \cap C_{I_i}(\beta, i)$ is disjoint for any $\beta \neq \alpha$ in $\mathbb{F}_q$.

Apart from the usual parameters: length, rate and minimum distance, the locality of a locally repairable code plays a crucial role. In this paper, we always consider locally repairable codes that are linear over $\mathbb{F}_q$. Thus, a $q$-ary locally repairable code of length $n$, dimension $k$, minimum distance $d$ and locality $r$ is said to be an $[n, k, d]_q$-locally repairable code with locality $r$.

If we ignore the minimum distance of a $q$-ary locally repairable code, then there is a constraint on the rate [7], namely,

$$\frac{k}{n} \leq \frac{r}{r+1}. \quad (2)$$

In this paper, the minimum distance of a locally repairable code is taken into consideration and we always refer to the bound (1). For an $[n, k, d]$-linear code, $k$ information symbols can recover the whole codeword. Thus, the locality $r$ is upper bounded by $k$. If we allow $r = k$, i.e., there is no constraint on locality, then the bound (1) becomes the usual Singleton bound that shows constraint on $n, k$ and $d$ only. The other extreme case is that the locality $r$ is 1. In this case, the locally repairable code is a repetition code by repeating each symbol twice and the bound (1) becomes $d(C) \leq n - 2k + 2$ which shows the Singleton bound for repetition codes.

B. The Rational Function Field and Its Automorphism Group

Let us introduce some basic facts of the rational function field. The reader may refer to [19] for more details.

Let $F$ be the rational function field $\mathbb{F}_q(x)$, where $x$ is transcendental over $\mathbb{F}_q$. There are exactly $q+1$ rational places of $F$, namely, the finite places $P_{x-\alpha}$ corresponding to $x - \alpha$ for all $\alpha \in \mathbb{F}_q$ and the infinity place $P_\infty$ corresponding to $1/x$. The set of places of $F$ is denoted by $\mathcal{P}_F$. Let $\nu_F$ be the normalized discrete valuation with respect to $P$. For a nonzero function $z$ of $F$, the zero divisor of $z$ is defined to
be defined to be $\sum_{p \in \mathbb{F}_q, v_p(z) > 0} v_p(z)P$, and the pole divisor of $z$ is defined to be $\sum_{p \in \mathbb{F}_q, v_p(z) < 0} v_p(z)P$. The principal divisor of $z$ is given by

$$
(z) = \sum_{p \in \mathbb{F}_q} v_p(z)P.
$$

We denote by $\text{Aut}(F/\mathbb{F}_q)$ the automorphism group of $F$ over $\mathbb{F}_q$, i.e.,

$$
\text{Aut}(F/\mathbb{F}_q) = \{ \sigma : F \to F \mid \sigma \text{ is an } \mathbb{F}_q\text{-automorphism of } F \}.
$$

It is well known that any automorphism $\sigma \in \text{Aut}(F/\mathbb{F}_q)$ is uniquely determined by $\sigma(x)$ and given by

$$
\sigma(x) = \frac{ax + b}{cx + d} \quad (3)
$$

for some constants $a, b, c, d \in \mathbb{F}_q$ with $ad - bc \neq 0$. Denote by $\text{GL}_2(q)$ the general linear group of $2 \times 2$ invertible matrices over $\mathbb{F}_q$. Thus, every matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(q)$ induces an automorphism of $F$ given by $(3)$. Two matrices of $\text{GL}_2(q)$ induce the same automorphism of $F$ if and only if they belong to the same coset of $Z(\text{GL}_2(q))$, where $Z(\text{GL}_2(q))$ stands for the center $\{aI_2 : a \in \mathbb{F}_q^* \}$ of $\text{GL}_2(q)$. This implies that $\text{Aut}(F/\mathbb{F}_q)$ is isomorphic to the projective general linear group $\text{PGL}_2(q) := \text{GL}_2(q)/Z(\text{GL}_2(q))$. Thus, we can identify $\text{Aut}(F/\mathbb{F}_q)$ with $\text{PGL}_2(q)$.

Consider a subgroup of $\text{PGL}_2(q)$:

$$
\text{AGL}_2(q) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{F}_q^* \text{ for } b \in \mathbb{F}_q \right\}.
$$

(4)

The group $\text{AGL}_2(q)$ is called the affine linear group. Every element $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{AGL}_2(q)$ induces an affine automorphism of $F$ determined by $\sigma(x) = ax + b$.

### C. The Subgroups of $\text{PGL}_2(q)$

As we need subgroups of $\text{PGL}_2(q)$ to construct optimal locally repairable codes in this paper, we have to find out subgroup structures of $\text{PGL}_2(q)$. It is fortunate that all subgroup structures of $\text{PGL}_2(q)$ are known. In this subsection, we present these known results.

By an easy counting argument, we know that the order of $\text{GL}_2(q)$ is $q^2 - 1)(q^2 - q)$. Thus, the order of $\text{PGL}_2(q)$ is $q(q^2 - 1)$ for each positive integer $1 \leq v \leq s - 1$, where

$$
\begin{align*}
\text{(v)} & \quad \text{if } q \text{ is a power of } \ell, \text{ there is one conjugacy class of } q(q^2 - 1)/(p^k - 1) \text{ conjugacy classes of } \text{subgroups that are isomorphic to } \text{PGL}_2(\ell). \\
\text{(vii)} & \quad \text{there are two conjugacy classes of cyclic subgroups of order } q \text{ when } q = p^s \text{ for } \text{any odd prime } p \text{ are listed as follows.}
\end{align*}
$$

(i) There are two conjugacy classes of cyclic subgroups of order 2.

(ii) There is one conjugacy class of $q(q \pm 1)/2$ cyclic subgroups of size $d$ for every divisor $d > 2$ of $(q \pm 1)$.

(iii) There are two conjugacy classes of $q(q^2 - 1)/6$ subgroups that are isomorphic to the dihedral group $D_4$ (or Klein 4-group).

(iv) There are two conjugacy classes of $q(q^2 - 1)/(2d)$ subgroups that are isomorphic to the dihedral group $D_{2d}$ of order $2d$ for every divisor $d > 2$ of $q^2 - 1$.

(v) There is one conjugacy class of $q(q^2 - 1)/(2d)$ subgroups that are isomorphic to the dihedral group $D_{2d}$ of order $2d$ for every divisor $d > 2$ of $(q \pm 1)$ such that $(q \pm 1)/d$ is an odd integer.

(vi) There are $q(q^2 - 1)/24$ subgroups isomorphic to $A_4$; $q(q^2 - 1)/24$ subgroups isomorphic to $S_4$, and $q(q^2 - 1)/60$ subgroups isomorphic to $A_5$ when $q \equiv \pm 1 (mod 10)$.

(vii) There is one conjugacy class of $q(q^2 - 1)/(2d)$ subgroups that are isomorphic to $\text{PGL}_2(\ell)$, where $q$ is a power of $\ell$.

(viii) $\text{PGL}_2(q)$ contains the subgroups $\text{PGL}_2(\ell)$, where $q$ is a power of $\ell$.

(ix) $\text{PGL}_2(q)$ contains the elementary abelian subgroups of order $p^s$ for $1 \leq v \leq s$. 

Furthermore, the subgroups in (vi) and (vii) are contained in the subgroup that are isomorphic to $\text{AGL}_2(q)$.
D. Hilbert's Ramification Theory

Let $F$ be the rational function field $\mathbb{F}_q(x)$. The full constant field of $F$ is $\mathbb{F}_q$ and the genus of $F$ is 0. For any subgroup $\mathcal{G}$ of $\text{Aut}(F/\mathbb{F}_q)$, let $F^G$ be the fixed subfield of $F$ with respect to $\mathcal{G}$, i.e.,

$$F^G = \{ y \in F : \sigma(y) = y \text{ for all } \sigma \in \mathcal{G} \}.$$  

By the Galois theory, $F/F^G$ is a finite Galois extension with $\text{Gal}(F/F^G) = \mathcal{G}$ [9, Theorem 11.36]. Since every subfield $E$ of $F$ with $\mathbb{F}_q \subseteq E \subseteq F$ is again a rational function field [19, Proposition 3.5.9], the genus of $F^G$ is $g(F^G) = 0$. Furthermore, the full constant field of $F^G$ is $\mathbb{F}_q$.

From the Hurwitz genus formula [19, Theorem 3.4.13], one has

$$2g(F) - 2 = |\mathcal{G}| - [2g(F^G) - 2] + \deg \text{Diff}(F/F^G),$$

where $g(F)$ stands for the genus of $F$ and $\text{Diff}(F/F^G)$ is the different of $F/F^G$. Let $Q$ be a place of $F^G$ and let $P_1, \ldots, P_t$ be all the places of $F$ lying over $P$. Then the ramification indices are $e_P(F/F^G)$ (resp. different exponents $d_P(F/F^G)$) of $P_i \mid Q$ are independent of $P_i$ for $1 \leq i \leq t$, and we can denote them by $e_Q(F/F^G)$ (resp. $d_Q(F/F^G)$). Hence, the degree of the different of $F/F^G$ can be given by

$$\deg \text{Diff}(F/F^G) = \sum_{P \in \mathbb{F}_q} d_P(F/F^G) \deg(P) = \sum_{Q \in \mathbb{F}_q} d_Q(F/F^G) e_Q(F/F^G) |\mathcal{G}| \cdot \deg(Q).$$

The $i$-th ramification group $\mathcal{G}_i(P)$ of $P \mid Q$ for each $i \geq 1$ is defined by

$$\mathcal{G}_i(P) = \{ \sigma \in \mathcal{G} : \nu_P(\sigma(z) - z) \geq i + 1 \text{ for all } z \in \mathcal{O}_P \},$$

where $\mathcal{O}_P$ is the valuation ring of $P$ in $F$. The different exponent $d_Q(F/F^G)$ can be calculated by

$$d_Q(F/F^G) = \sum_{i=0}^{\infty} (|\mathcal{G}_i(P)| - 1)$$

from Hilbert’s Different Theorem [19, Theorem 3.8.7]. Furthermore, we have the following ramification structures for the rational function field [9, Theorem 11.92].

**Proposition II.3.** Let $F$ be the rational function field $\mathbb{F}_q(x)$. Denote by $A$ the automorphism group $\text{Aut}(F/\mathbb{F}_q)$, then the extension $F/F^A$ has the following properties.

(i) Every rational place $P$ of $F$ is wildly ramified in $F/F^A$; $\mathcal{G}_1(P)$ is the semidirect product of an elementary abelian $p$-group of order $q - 1$ with a cyclic group of order $q - 1$; $\mathcal{G}_2(P)$ is an elementary abelian $p$-group of order $q$ and $\mathcal{G}_3(P)$ is trivial for any $i \geq 2$. Furthermore, all rational places form a single orbit of size $q + 1$ under the group action of $A$ on the set of places of $F$.

(ii) Every place $Q$ of degree 2 of $F$ is tamely ramified in $F/F^A$; $\mathcal{G}_0(Q)$ is a cyclic group of order $q + 1$. Furthermore, all places of degree 2 form a single orbit of size $(q^2 - q)/2$ under the group action of $A$ on the set of places of $F$.

(iii) Other places of $F$ are unramified in $F/F^A$.

In fact, one can explicitly compute all the ramification groups of rational places and places of degree 2. For instance, let $P_\infty$ be the pole of $x$. Then $\mathcal{G}_{-1}(P_\infty) = \mathcal{G}_0(P_\infty) = \text{AGL}_2(q)$ and $\mathcal{G}_1(P_\infty)$ is isomorphic to the group $\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_q \right\} \cong (\mathbb{F}_q, +)$.

E. Algebraic Geometry Codes

In this subsection, we introduce a modification of the algebraic geometry codes. The reader may refer to [14], [22], [23] for more details on algebraic geometry codes.

Let $F$ be the rational function field $\mathbb{F}_q(x)$. Let $G$ be a divisor of $F$. The Riemann-Roch space associated to $G$ is defined by

$$\mathcal{L}(G) = \{ z \in F^* : \deg(z) \geq -G \} \cup \{ 0 \}.$$

It is a finite-dimensional vector space over $\mathbb{F}_q$ and its dimension $\ell(G)$ is lower bounded by $\ell(G) \geq \deg(G) + 1$ from Riemann’s theorem [19, Theorem 1.4.17]. Furthermore, the equality holds true if $\deg(G) \geq 1$. Let $\mathcal{P} = \{ P_1, \ldots, P_n \}$ be a set of $n$ distinct rational places of $F$. For a special divisor $G$ with $0 < \deg(G) < n$ and $\text{supp}(G) \cap \mathcal{P} = \emptyset$, the algebraic geometry code is defined to be

$$C(\mathcal{P}, G) := \{ (f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G) \}.$$  

Then $C(\mathcal{P}, G)$ is an $[n, \deg(G) + 1, n - \deg(G)]$-MDS code. If $V$ is a subspace of $\mathcal{L}(G)$, we can define a subspace of $C(\mathcal{P}, G)$ by

$$C(\mathcal{P}, V) := \{ (f(P_1), \ldots, f(P_n)) : f \in \mathcal{V} \}.$$  

The code $C(\mathcal{P}, V)$ is usually no longer an MDS code, but the minimum distance is still lower bounded by $n - \deg(G)$.

For the purpose of our paper, we need to modify the above construction. We can remove the condition that $\text{supp}(G) \cap \mathcal{P} = \emptyset$. Assume that $G$ is a divisor of $F$ and let $m_i = \nu_{P_i}(G)$. Choose a local parameter $\pi_i$ of $P_i$ for each $i \in \{ 1, 2, \ldots, n \}$. Then for any nonzero function $f \in \mathcal{L}(G)$, we have $\nu_{P_i}(\pi_i^m f) = m_i + \nu_{P_i}(f) \geq m_i - \nu_{P_i}(G) = 0$. Define a modified algebraic geometry code as follows

$$C(\mathcal{P}, G) := \{ (\pi_1^{m_1} f(P_1), \ldots, (\pi_n^{m_n} f(P_n)) : f \in \mathcal{L}(G) \}.$$  

We claim that $C(\mathcal{P}, G)$ is still an $[n, \deg(G) + 1, n - \deg(G)]$-MDS code in this case. It is sufficient to show that the Hamming weight of the codeword

$$((\pi_1^{m_1} f(P_1), \ldots, (\pi_n^{m_n} f(P_n))$$

is at least $n - \deg(G)$ for every nonzero function $f \in \mathcal{L}(G)$. Let $I$ be the subset of $\{ 1, 2, \ldots, n \}$ such that $(\pi_i^{m_i} f(P_i)) = 0$. Then we have $f \in \mathcal{L}(G - \sum_{i \in I} P_i)$. 


Thus, \( \deg(G - \sum_{i \in I} P_i) \geq 0 \), i.e., \(|I| \leq \deg(G) \). This gives a lower bound \( n - |I| \geq n - \deg(G) \) on the Hamming weight of the codeword. Now, for a subspace \( V \) of \( \mathcal{L}(G) \), we can define a subcode of \( (P, G) \) by

\[
C(P, V) := \{(\pi_1^{m_1} f)(P_1), \ldots, (\pi_n^{m_n} f)(P_n) : f \in V\}. \tag{9}
\]

Again, the minimum distance of \( C(P, V) \) is lower bounded by \( n - \deg(G) \).

**III. GENERAL CONSTRUCTION OF OPTIMAL LRC CODES**

The idea of our construction works as follows. Let \( F \) be the rational function field \( \mathbb{F}_q(x) \). Let \( G \) be a subgroup of \( \text{Aut}(F/\mathbb{F}_q) \), of order \( r+1 \). Then there is a subfield \( E \) of \( F \) such that \( F/E \) is a Galois extension with Galois group \( \text{Gal}(F/E) = G \). Now assume that \( Q_1, Q_2, \ldots, Q_m \) are rational places of \( E \) and they are all splitting completely in the extension \( F/E \). Let \( P_{i1}, P_{i2}, \ldots, P_{ir+1} \) denote the \( r+1 \) rational places of \( F \) that lie over \( Q_i \) for each \( 1 \leq i \leq m \). Put \( n = (r+1)m + r \) and put \( \mathcal{P} = \{P_i \}|_{1 \leq i \leq m, 1 \leq j \leq r+1} \). Choose a divisor \( D \) of degree \( k+r-2 \) with \( k = rt \) for some integer \( 1 \leq t \leq m \), a function \( z \) of \( E \) with \( \deg(z) = 1 \) (here \( z \) is the pole divisor of \( z \) in \( E \)) and a function \( x \) of \( F \) with \( \deg(x) = 1 \). Then the code \( \{ (f(P))_{P \in \mathcal{P}} : f \in \sum_{i=1}^m \left( \sum_{j=0}^k a_{ij} z^j \right) x^i : a_{ij} \in \mathbb{F}_q \} \) is an optimal \( q \)-ary \([n, k, d]\)-locally repairable code with locality \( r \), \( k = rt \) and \( d = n - k - k + 2 \) (see the proof of Proposition III.1 below).

Apparently, to construct optimal locally repairable codes using this idea, one has to analyze the splitting behavior of places of \( E \) in \( F \). In order to do so, we need to know the explicit structure of \( G \). As all subgroup structures are given in Propositions II.1 and II.2, we are able to produce optimal locally repairable codes from an arbitrary subgroup of \( \text{PGL}_2(q) \). On the other hand, it is unnecessary to provide explicit constructions from all subgroups of \( \text{PGL}_2(q) \) one by one. Instead, in this section, we give a general construction of optimal locally repairable codes for all subgroups of automorphism group of the rational function field by estimating the number of ramified rational places in \( F \). Explicit constructions corresponding to subgroups of the affine linear group \( \text{AGL}_2(q) \), the cyclic group of size \( q+1 \) and dihedral groups are provided in the following sections.

**Proposition III.1.** Assume that there is a subgroup of \( \text{PGL}_2(q) \), of order \( r+1 \) with \( 1 \leq r \leq \frac{q}{2} \). Put \( n = m(r+1) \) for any positive integer \( m \leq \left\lfloor \frac{q-1}{2(r+1)} \right\rfloor \). Then, for any integer \( t \) with \( 1 \leq t \leq m \), there exists an optimal \( q \)-ary \([n, k, d]\)-locally repairable code with locality \( r \), \( k = rt \) and \( d = n - k - k + 2 \).

**Proof:** Let \( F \) be the rational function field over \( \mathbb{F}_q \). Assume that there exists a subgroup \( G \) of \( \text{Aut}(F/\mathbb{F}_q) \) of order \( r+1 \). Denote by \( \{R_1, R_2, \ldots, R_t\} \) the set of all rational places of \( F \) which are ramified in \( F/F^G \). By the Hurwitz genus formula, we have

\[
2g(F) - 2 \geq (r+1)[2g(F^G) - 2] + \sum_{i=1}^t d_{R_i}(F/F^G) \deg(R_i)
\]

\[
\geq -2(r+1) + s.
\]

This gives \( s \leq 2r \). Hence, there are at least \( q + 1 - s \geq q + 1 - 2r \geq m(r+1) \) rational places of \( F \) which are unramified in \( F/F^G \). Let \( P \) be a rational place of \( F \) which is unramified in \( F/F^G \) and let \( Q \) be its restriction to \( F^G \). Then we have ramification index \( e(P|Q) = 1 \) and relative degree \( f(P|Q) = [O_P/P : O_Q/Q] = [F: F_Q] = 1 \). Hence, there are \( m \) rational places \( \{Q_1, Q_2, \ldots, Q_m\} \) of \( F^G \) which split completely in \( F/F^G \) by fundamental equality [19, Theorem 3.11]. Denote by \( \mathcal{P} = \{P_1, P_2, \ldots, P_n\} \) the set of rational places of \( F \) lying over \( \{Q_1, Q_2, \ldots, Q_m\} \).

Let \( P_\infty \) be a rational place of \( F \) such that \( P_\infty \notin \mathcal{P} \). Then there exists an element \( x \in F \) such that \( (x) = P_\infty \) and \( F = F_\infty \) [19, Proposition 1.6.6]. Let \( Q_\infty \) be the restriction of \( P_\infty \) to \( F^G \). Similarly, there exists an element \( z \in F^G \) such that \( (z)^{F_\infty} = Q_\infty \) and \( F^G = F_\infty(z) \). Thus, \( \supp((z)) \cap \mathcal{P} = \emptyset \) and \( \deg((z)) \leq [F : F^G] = r + 1 \).

For \( r \geq 1 \), consider the set of functions

\[
V := \left\{ \sum_{i=0}^{r-1} \left( \sum_{j=0}^{t-1} a_{ij} z^j \right) x^i : a_{ij} \in \mathbb{F}_q \right\}.
\]

First of all, as \( \mathbb{F}_q(x) : \mathbb{F}_q(z) = r + 1 \), the set \( \{1, x, \ldots, x^{r-1}\} \) is linearly independent over \( \mathbb{F}_q(z) \). Thus, the vector space \( V \) has dimension \( rt \) over \( \mathbb{F}_q \). Consider the subcode of the algebraic geometry code

\[
C(P, V) = \{(f(P_1), \ldots, f(P_n)) : f \in V\}.
\]

Then we claim that \( C(P, V) \) is an optimal \([n, k, d]\)-locally repairable code with locality \( r \), \( k = rt \) and \( d = n - k - k + 2 \).

Firstly, it is clear that \( C(P, V) \) is an \( \mathbb{F}_q \)-linear code of length \( n \). For every nonzero function \( f \in V \), the pole divisor of \( f \) is at most \((t-1)(r+1) + (r-1)(1) = 2t(r-1) - 2 \), i.e., \( f \) has at most \((r+1)t-2 \) zeros. This implies that the Hamming weight of \( \text{supp}(\{f(P_1), \ldots, f(P_n)\}) \) is at least \( n - rt - r + 2 = n - k - k + 2 > 0 \). Therefore, the dimension of \( C(P, V) \) is \( k = rt \) and its minimum distance is \( d = n - k - k + 2 \). By the Singleton-type bound (1), we obtain \( d = n - k - k + 2 \) if \( C(P, V) \) has locality \( r \).

It remains to prove that \( C(P, V) \) has locality \( r \). We claim that \( x(P_a) \neq x(P_b) \) for any two different rational places \( P_a, P_b \in \mathcal{P} \). Otherwise, \( x - c \) would have two zeros \( P_a \) and \( P_b \), where \( c = x(P_a) = x(P_b) \in \mathbb{F}_q \). Thus, \( \deg(x-c) > 0 \). This is a contradiction to the fact that \( \deg(x-c) = \deg(x-c) = \deg(x) = 1 \).

Let \( A_t \) be the set of rational places of \( F \) which lie over \( Q_\ell \) for \( 1 \leq \ell \leq m \). Suppose that the erased symbol of codeword is \( c_0 = f(P_a) \), where \( P_a \in A_t \). Put \( b_i = \sum_{j=0}^{r-1} a_{ij} z^j(P_a) \) for \( 0 \leq i \leq r-1 \), as \( z \) is a function of \( F^G \), we have \( z(P_b) = z(P_a) \) for all \( \beta \in A_t \). Hence, for all \( P_a, P_b \in A_t \), we have

\[
f(P_b) = \sum_{i=0}^{r-1} \left( \sum_{j=0}^{r-1} a_{ij} z^j(P_b) \right) x^i(P_b) = \sum_{i=0}^{r-1} b_i x^i(P_b).
\]
Define the decoding polynomial \( \delta(x) = \sum_{i=0}^{r-1} b_i x^i \). Then we have

\[
\delta(x)(P_\beta) = \sum_{i=0}^{r-1} b_i x^i(P_\beta) = f(P_\beta).
\]

Since \( \delta(x) \) is a polynomial of degree at most \( r - 1 \) and \( \{x(P_\beta)\}_{P_\beta \in \mathcal{A}_I \setminus \{P_i\}} \) are pairwise distinct, it can be interpolated from these \( r \) symbols \( c_\beta = f(P_\beta) \) for \( P_\beta \in \mathcal{A}_I \setminus \{P_i\} \). Hence, the erased symbol \( c_\alpha = \delta(x)(P_\alpha) \) can be recovered by the Lagrange interpolation. This completes the proof. \( \blacksquare \)

**Remark 1.** The concept of locally repairable codes can be extended to codes with multiple erasures. A code \( C \subset \mathbb{F}_q^n \) of size \( q^k \) is said to be an \((n, r, k, \rho)\) locally repairable code if each coordinate \( i \in [n] \) is contained in a subset \( I_i \subset [n] \) of size at most \( r + \rho - 1 \) such that the restriction \( C|_{I_i} \) to the coordinates in \( I_i \) forms a code of minimum distance at least \( \rho \). Furthermore, the minimum distance of \((n, k, r, \rho)\) locally repairable codes is upper bounded by \( \left\lceil \frac{n}{r} \right\rceil - 1 \) \((\rho - 1)\).

If we assume that the order of \( G \) is \( r + \rho - 1 \) and let \( V \) be defined as in the proof of Proposition III.1, then we can show that there exists a \( q \)-ary \((n, k, r, \rho)\) locally repairable code with \( n = (r + \rho - 1)m \), \( k = rt \) and \( \rho \geq n - (r + \rho - 1)(t - 1) - (r - 1) = n - k - 1 - \left\lceil \frac{k}{r} \right\rceil - 1 \) \((\rho - 1)\). Hence, we can construct locally repairable codes with multiple erasures from automorphism group of the rational function field as well.

Combining Proposition III.1 with Propositions II.1 and II.2, we can immediately obtain the following optimal locally repairable codes.

**Theorem III.2.** If a positive integer \( r \leq \frac{q}{4} \) satisfies one of the following conditions, then for any positive integer \( n \leq (r + 1)\left\lceil \frac{q+1+2r}{r+1} \right\rceil \) that is divisible by \( r + 1 \) and any integer \( t \geq 1 \), there exists an optimal \( q \)-ary \([n, k, d]\)-locally repairable code with locality \( r \), \( k = rt \) and \( d = n - k - \frac{k}{r} + 2 \).

(i) \( r + 1 \) is a divisor of \( q - 1 \);

(ii) \( r + 1 \) is a divisor of \( q \);

(iii) \( r + 1 \equiv u \mod v \), where \( u \geq 2 \), \( v \geq 1 \) and \( u \) is a common divisor of \( q - 1 \) and \( p^2 - 1 \);

(iv) \( r + 1 \) is a divisor of \( q + 1 \);

(v) \( r + 1 = 2h \), where \( h \geq 2 \) is a divisor of \( q + 1 \) for even \( q \) or \( \frac{q+1}{2} \) for odd \( q \);

(vi) \( r + 1 = \ell t - 1 \), where \( q \) is odd and \( \ell \) is a power of \( \ell \);

(vii) \( r + 1 = \ell (t^2 - 1) / 2 \), where \( q \) is odd and \( \ell \) is a power of \( \ell \);

(viii) \( r + 1 = 12 \), if \( q \) is an even power of 2 or \( q \) is odd;

(ix) \( r + 1 = 24 \), if \( q \) is odd;

(x) \( r + 1 = 60 \), if \( q \) is an even power of 2 or \( q \equiv \pm 1 \mod 10 \).

**Remark 2.** The advantage of Theorem III.2 is that one can produce optimal \( q \)-ary locally repairable codes without knowing explicit structures of subgroups of \( PGL_2(q) \), while the disadvantage of Theorem III.2 is that it is an existence result.

**Remark 3.** For a subgroup \( G \) of \( \text{Aut}(F/\mathbb{F}_q) \) of order \( r + 1 \), let \( s \) be the number of rational places of \( F \) which are ramified in \( F/F^G \) (see [9, Theorem 11.91]). Then, the length \( n \) of the optimal locally repairable codes can be as large as \( q + 1 - s \).

In the following sections, we will construct optimal locally repairable codes explicitly by analyzing subgroup structures of \( \text{Aut}(F/\mathbb{F}_q) \).

Let us look at some examples by plugging some values of \( q, r, t \) and \( n \) in Theorem III.2.

**Example III.3.** (i) Let \( q = 27 \). Then for \( r \in \{1, 2, 3, 5, 6, 8\} \), there is a subgroup of \( PGL_2(27) \) of order \( r + 1 \). Thus, for \( n = (r + 1)\left\lceil \frac{28 - 2r}{r+1} \right\rceil \) and any integer \( t \geq 1 \), there exists an optimal \( q \)-ary \([n, k, d]\)-locally repairable code with locality \( r \), \( k = rt \) and \( d = n - k - \frac{k}{r} + 2 \). For instance, for \( r = 2 \), there exists an optimal 27-ary code for locality \( 3 \) for any \( 1 \leq t \leq 8 \). If we take \( r = 3 \), we obtain an optimal 27-ary code with locality \( 3 \) for any \( 1 \leq t \leq 5 \).

(ii) Let \( q = 64 \). Then for \( r \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 15, 17, 20\} \), there is a subgroup of \( PGL_2(64) \) of order \( r + 1 \). Thus, for \( n = (r + 1)\left\lceil \frac{65 - 2r}{r+1} \right\rceil \) and any integer \( t \geq 1 \), there exists an optimal \( q \)-ary \([n, k, d]\)-locally repairable code with locality \( r \), \( k = rt \) and \( d = n - k - \frac{k}{r} + 2 \). For instance, for \( r = 3 \), there exists an optimal 64-ary code for locality \( 3 \) for any \( 1 \leq t \leq 14 \). If we let \( r = 5 \), then there exists an optimal 64-ary code for locality \( 5 \) for any \( 1 \leq t \leq 9 \).

**Remark 4.** It is easy to see that the optimal locally repairable codes with locality \( r = 6 \) for \( q = 27 \) and locality \( r = 4, 9, 12 \) for \( q = 64 \) can’t be obtained from the construction of Tam and Barg in [20].

By Proposition III.1, Propositions II.1 and II.2, we can give a result on some small locality for locally repairable codes over finite fields of small characteristics.

**Corollary III.4.** If a pair \((q, r)\) of positive integers satisfies one of the following conditions, then for any positive integer \( n \leq (r + 1)\left\lceil \frac{q+1+2r}{r+1} \right\rceil \) that is divisible by \( r + 1 \) and any integer \( t \geq 1 \), there exists an optimal \( q \)-ary \([n, k, d]\)-locally repairable code with locality \( r \), \( k = rt \) and \( d = n - k - \frac{k}{r} + 2 \).

(i) \( q = 2^g \) with \( s \geq 4 \) and \( r \in \{1, 2, 5\} \);

(ii) \( q = 3^g \) with \( s \geq 4 \) and \( r \in \{1, 2, 3, 4, 5, 11, 23\} \);

(iii) \( q = 4^g \) with \( s \geq 3 \) and \( r \in \{1, 2, 3, 5, 9, 11\} \);

(iv) \( q = 5^g \) with \( s \geq 3 \) and \( r \in \{1, 2, 3, 4, 5, 9, 11, 19, 23\} \).

**Proof:** (i) follows from Proposition III.1 and the fact that \( PGL_2(q) \) contains the group \( PGL_2(2) \) and \( PGL_2(2) \) contains subgroups of order 2, 3 and 6.

(ii) For \( q = 3^g \) with \( s \geq 4, 2(q - 1), 3(q, 4)(q - 1) \) for even \( s \) or \( 4(q + 1) \) for odd \( s \). Thus, there is a subgroup of \( PGL_2(q) \) of order \( r + 1 \) for \( r \in \{1, 2, 3\} \). There is also an affine subgroup of order 6 since \( 2(3 - 1) \) from Theorem III.2(ii). The order of \( A_4 \) is 12, and the order of \( PGL_2(3) \) is 24.
There is a subgroup of $\text{PGL}_2(q)$ of order $r + 1$ for $r \in \{1, 2, 3, 4, 5, 9, 11\}$ since $2|q$, $3|(q - 1)$, $4|q$, $5|(q - 1)$ for even $s$ or $5|q + 1$ for odd $s$; the order of $\text{PGL}_2(2)$ is 6; there is a dihedral subgroup of order 10 from Theorem III.2(v); and the order of $A_4$ is 12.

There is a subgroup of $\text{PGL}_2(q)$ of order $r + 1$ for $r \in \{1, 2, 3, 4, 5, 9, 11, 19, 23\}$ since both 2 and 4 are divisors of $q - 1$; both 3 and 6 are divisors of $q - 1$ for even $s$ or $q + 1$ for odd $s$; 5|$q$; there are affine subgroups of order 10 and 20, respectively, since 2|$5(5 - 1)$ and 4|$5(5 - 1)$ from Theorem III.2(iii); the order of $A_4$ is 12; and the order of $S_4$ is 24.

IV. Explicit Construction via Affine Subgroups

In the previous section, we provided a construction for arbitrary subgroups of $\text{PGL}_2(q)$ by estimating the number of ramified rational places. From this section onwards, we will consider some particular subgroups and analyze ramifications of rational places.

In this section, we will construct optimal locally repairable codes from subgroups of the affine linear group $\text{AGL}_2(q)$. It turns out that the optimal locally repairable codes constructed by Tamo and Barg in [20] are examples in this section. More precisely, we will see that the construction given in [20] is equivalent to the construction via affine linear group under our framework.

Let $\mathbb{F}_q$ be the finite field with $q = p^s$ elements and let $F$ be the rational function field $\mathbb{F}_q(x)$. The proof of the following proposition provides explicit group structures of $\text{AGL}_2(q)$.

**Proposition IV.1.** Let $q = p^s$. Let $\nu$ be an integer with $0 \leq \nu \leq s$ and let $u$ be a common divisor of $q - 1$ and $p^\nu - 1$. Then there is a subgroup $G$ of $\text{AGL}_2(q)$ of order $up^\nu$.

**Proof:** If $u$ is a divisor of $q - 1$, then there exists a subgroup $H$ of the multiplicative group $\mathbb{F}_q^*$ of order $u$. As $u|(p^\nu - 1)$, the field $\mathbb{F}_p(H)$ is contained in $\mathbb{F}_p$. Put $\ell = \min\{r > 0 : u|(p^r - 1)\}$. Then we have $\mathbb{F}_p(H) = \mathbb{F}_p$ and $\ell = \gcd(u, s)$.

Let $W$ be a vector subspace of $\mathbb{F}_q$ over $\mathbb{F}_p$ with dimension $\nu/\ell$. Put

$$ G := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in H, \ b \in W \right\}. $$

(10)

Then it is easy to verify that $G$ is a subgroup of $\text{AGL}_2(q)$ of order $up^\nu$.

The ramification information of the $F/F^G$ are provided in the following proposition. In particular, the number of ramified rational places of $F$ in the extension $F/F^G$ can be determined.

**Proposition IV.2.** Let $q = p^s$. Let $\nu$ be an integer with $0 \leq \nu \leq s$ and let $u$ be a common divisor of $q - 1$ and $p^\nu - 1$. Let $G$ be a subgroup of $\text{AGL}_2(q)$ of order $up^\nu$ that is defined in Equation (10). Then the extension $F/F^G$ has the following properties.

(i) $|F : F^G| = up^\nu$.

(ii) The infinity place $P_\infty$ of $F$ is totally ramified in $F/F^G$ with ramification index $e_{P_\infty}(F/F^G) = up^\nu$ and different exponent $d_{P_\infty}(F/F^G) = up^\nu + p^\nu - 2$, where $P_\infty$ is the unique pole of $x$. There is a rational place of $F^G$ which splits into $p^\nu$ rational places $\{P_1, P_2, \ldots, P_{p^\nu}\}$ of $F$. Each place $P_i$ has ramification index $e_{P_i}(F/F^G) = u$ and different exponent $d_{P_i}(F/F^G) = u - 1$. Theorem IV.3

(iii) The unique zero of $x$ is ramified in $F/F^G$ with ramification index $u$ if $u > 1$. Hence, $P_0 \in \{P_1, P_2, \ldots, P_{p^\nu}\}$.

(iv) Other places of $F$ are unramified in $F/F^G$.

**Proof:** (i) is clear by Galois theory.

To prove (ii), let $\mathcal{A}$ denote the automorphism group $\text{Aut}(F/F^G)$. From Proposition II.3 and the paragraph after Proposition II.3, we know that the inertia group of the infinite place $P_\infty$ in $F/F^G$ is $\text{AGL}_2(q)$. Thus, the infinite place $P_\infty$ is totally ramified in $F/F^G$. Since $G$ is a subgroup of $\text{AGL}_2(q)$, $P_\infty$ is totally ramified in $F/F^G$, i.e., $e_{P_\infty}(F/F^G) = up^\nu$. It is straightforward to verify that the orders of ramification groups of $P_\infty$ in $F/F^G$ are given by $|\mathcal{A}(P_\infty)| = up^\nu$, $|\mathcal{A}(P_0)| = p^\nu$ and $|\mathcal{A}(P_\infty)| = 1$ for $i > 1$.

Hence, the different exponent is $d_{P_\infty}(F/F^G) = up^\nu + p^\nu - 2$ from Hilbert’s Different Theorem. Assume that $Q_1, Q_2, \ldots, Q_k$ are the remaining ramified places of $F^G$ in $F/F^G$ with ramification indices $e_i$ and different exponents $d_i$ for $1 \leq i \leq k$.

Form the Hurwitz genus formula, one has

$$ 2g(F) - 2 = |G| \cdot [2g(F^G) - 2] + up^\nu + p^\nu - 2 + \sum_{i=1}^{k} \frac{d_i}{e_i} \cdot |G| \cdot \deg(Q_i). $$

(11)

Since any fixed subfield of the rational function field is again a rational function field, we have $g(F) = g(F^G) = 0$. Hence, it follows from (11) that

$$ \sum_{i=1}^{k} \frac{d_i}{e_i} \cdot \deg(Q_i) = \frac{u - 1}{u}. $$

(12)

If $u = 1$, then $k = 0$. Otherwise we must have $k = 1$, $e_1 = u$, $\deg(Q_1) = 1$ and this rational place $Q_1$ splits into at most $p^\nu$ places in $F$ from fundamental equality. Since the rational places of $F$ have relative degree 1 in the extension $F/F^G$, there are $(q - p^\nu)/(up^\nu)$ rational places of $F^G$ that split completely in $F/F^G$. Furthermore, $Q_1$ splits into $p^\nu$ rational places in $F$.

Again, it is straightforward to verify that the orders of ramification groups of $P_0$ in $F/F^G$ are given by $|\mathcal{A}(P_0)| = u$, and $|\mathcal{A}(P_0)| = 1$ for $i > 1$. Thus, $P_0$ is ramified in $F/F^G$ with ramification index $u$. This proves (iii).

(iv) follows from the proof of (ii).

Now we can provide explicit constructions of optimal locally repairable codes from subgroups of $\text{AGL}_2(q)$.

**Theorem IV.3.** Let $q = p^s$. Let $\nu$ be a positive integer less than or equal to $s$. Put $r = p^{\nu - 1}$ and $n = m(r + 1)$ for any positive integer $m \leq q/(r + 1)$. Then for any integer $t$ with $1 \leq t \leq m$, there exists an optimal $q$-ary $[n, k, d]$-locally repairable code with locality $r$, $k = rt$ and $d = n - k - \frac{n}{2} + 2$. 
Proof: Let $F$ be the rational function field $\mathbb{F}_q(x)$ and let $P_\infty$ be the infinite place of $F$, i.e., $(x)_\infty = P_{\infty}$. Let $G$ be the subgroup of $\text{AGL}_2(q)$ with order $r + 1 = p^0$ constructed from Equation (10). Then by Proposition IV.2, except for $P_{\infty}$ all other $q$ rational places of $F$ split completely. Denote by $\mathcal{P}$ a set of $m(r + 1)$ rational places of $F$ that lie over $m$ rational places of $F^G$.

Let $Q_\infty$ be the place of $F^G$ that lies under $P_{\infty}$ and choose an element $z \in F^G$ such that $(z)_\infty$ is equal to $Q_\infty$ as a divisor of $F^G$. Thus, $(z)_\infty$ is equal to $(r + 1)P_{\infty}$ as a divisor of $F$.

For $t \geq 1$, consider the set of functions

$$V := \left\{ \sum_{j=0}^{t} \sum_{j=0}^{r-1} a_{ij} z^j \mid x^j : a_{ij} \in \mathbb{F}_q \right\}.$$ 

Then by mimicking the proof of Proposition III.1, one can show that the code $C(\mathcal{P}, V)$ is an optimal $q$-ary $[n, k, d]$-locally repairable code with locality $r$, $k = rt$ and $d = n - k - \frac{r}{t} + 2$.

Remark 5. In the proof of Theorem IV.3, one can choose the function $z$ to be $\prod_{b \in W}(x + b)$, where $W$ is the $\mathbb{F}_p$-vector space of dimension $v$ used to define $G$ in Equation (10). Then Theorem IV.3 provides the same construction as the one using additive subgroups in [20, Proposition 3.2].

In Theorem IV.3, we make use of a subgroup $G$ of $\text{AGL}_2(q)$ that is isomorphic to an additive subgroup of $\mathbb{F}_q$. The following theorem will use a subgroup $G$ of $\text{AGL}_2(q)$ that is isomorphic to a multiplicative subgroup of $\mathbb{F}_q^*$.

**Theorem IV.4.** Let $r$ be a positive integer with $(r + 1)(q - 1)$. Put $n = m(r + 1)$ for any positive integer $m \leq (q - 1)/(r + 1)$. Then for any integer $t$ with $1 \leq t \leq m$, there exists an optimal $[n, k, d]_q$-locally repairable code with locality $r$, $k = rt$ and $d = n - k - \frac{r}{t} + 2$.

**Proof:** Let $F$ be the rational function field $\mathbb{F}_q(x)$ and let $P_\infty$ be the unique pole of $x$, i.e., $(x)_\infty = P_{\infty}$. Let $G$ be a subgroup of $\text{AGL}_2(q)$ of order $r + 1$ constructed from Equation (10). Then by Proposition IV.2, except for $P_{\infty}$ and the zero of $x$, all other $q - 1$ rational places of $F$ split completely. Denote by $\mathcal{P}$ a set of $m(r + 1)$ rational places of $F$ that lie over $m$ rational places of $F^G$.

Let $Q_\infty$ be the place of $F^G$ that lies under $P_{\infty}$ and choose an element $z \in F^G$ such that $(z)_\infty$ is equal to $Q_\infty$ as a divisor of $F^G$. Thus, $(z)_\infty$ is equal to $(r + 1)P_{\infty}$ as a divisor of $F$.

For $t \geq 1$, consider the set of functions

$$V := \left\{ \sum_{j=0}^{t-1} \sum_{j=0}^{r-1} a_{ij} z^j \mid x^j : a_{ij} \in \mathbb{F}_q \right\}.$$ 

Then by mimicking the proof of Proposition III.1, one can show that the code $C(\mathcal{P}, V)$ is an optimal $[n, k, d]_q$-locally repairable code with locality $r$, $k = rt$ and $d = n - k - \frac{r}{t} + 2$.

Remark 6. In the proof of Theorem IV.3, one can choose the function $z$ to be $\prod_{b \in H} x = x^{r+1}$, where $H$ is the subgroup of $\mathbb{F}_q^*$ used to define $G$ in Equation (10). Then Theorem IV.4 provides the same construction as the one using multiplicative subgroups in [20, Proposition 3.2].

Now we consider subgroups of $\text{AGL}_2(q)$ that mix additive subgroups of $\mathbb{F}_q$ and multiplicative subgroups of $\mathbb{F}_q^*$.

**Theorem IV.5.** Let $q \geq 2$ be a common divisor of $q - 1$ and $p^0 - 1$ for some $1 \leq b \leq s$. Let $r$ be a positive integer such that $r + 1 = qp^0$. Put $n = m(r + 1)$ for any positive integer $m \leq (q - p^0)/(qp^0)$. Then for any integer $t$ with $1 \leq t \leq m$, there exists an optimal $[n, k, d]_{q^t}$-locally repairable code with locality $r$, $k = rt$ and $d = n - k - \frac{r}{t} + 2$.

One can imitate the proof of Theorem IV.3 or Theorem IV.4 by considering a subgroup of $\text{AGL}_2(q)$ of size $up^0$ defined in Equation (10). One can choose the function $z$ to be $z = \prod_{a \in H, b \in W}(ax + b)$, where $H, W$ are used to define $G$ in the Equation (10). We skip the details.

**Example IV.6.** (i) Let $q = 27$. If we let $r = 2$ and $m = 9$ in Theorem IV.3, then we can explicitly construct an optimal 27-ary $[27, 2r, 29 - 3r]$-locally repairable code with locality 2 for any $1 \leq t \leq 9$. Note that the code length gets enlarged compared with Example III.3(i). This is because we know the ramification information. If we let $r = 12$ and $m = 2$ in Theorem IV.4, then we can explicitly construct an optimal 27-ary $[26, 12r, 28 - 13r]$-locally repairable code with locality 12 for any $1 \leq t \leq 2$. If we let $r = 5$ and $m = 4$ in Theorem IV.5, then we can explicitly construct an optimal 27-ary $[24, 5r, 26 - 6r]$-locally repairable code with locality 5 for any $1 \leq t \leq 4$.

(ii) Let $q = 64$. If we let $r = 3$ and $m = 16$ in Theorem IV.3, then we can explicitly construct an optimal 64-ary $[64, 3r, 66 - 4r]$-locally repairable code with locality 3 for any $1 \leq t \leq 16$. Note that the code length gets enlarged compared with Example III.3(i). If we let $r = 8$ and $m = 7$ in Theorem IV.4, then we can explicitly construct an optimal 64-ary $[63, 8r, 65 - 9r]$-locally repairable code with locality 8 for any $1 \leq t \leq 7$. If we let $r = 11$ and $m = 5$ in Theorem IV.5, then an optimal 64-ary $[60, 11r, 62 - 12r]$-locally repairable code with locality 11 for any $1 \leq t \leq 5$ can be constructed.

V. **Explicit Construction of LRC Codes of Length $n = q + 1$**

In this section, we give an explicit construction of optimal locally repairable codes of length $n = q + 1$ via subgroups of a cyclic group of order $q + 1$ in $\text{Aut}(F/\mathbb{F}_q)$. First of all, we provide an explicit characterization of fixed subfields of the rational function field $\mathbb{F}_q(x)$ with respect to subgroups of a cyclic group of order $q + 1$.

**Lemma V.1.** Let $F$ be the rational function field $\mathbb{F}_q(x)$. Let $f(x)$ be a quadratic primitive polynomial $x^2 + ax + b \in \mathbb{F}_q[x]$ of order $q^2 - 1$. Let $\sigma$ be the automorphism of $F$ determined by $\sigma(x) = 1/(-bx - a)$. Then the order of $\sigma$ is $q + 1$. Furthermore, let $G$ be a subgroup of $\langle \sigma \rangle$ and let $\text{Tr}(x) = \sum_{\tau \in G} \tau(x)$, then we have $F^G = \mathbb{F}_q(\text{Tr}(x))$.

**Proof:** Let $A_f = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix}$ be the companion matrix of the quadratic primitive polynomial $x^2 + ax + b$. We claim
that $A_f$ has order $q + 1$ in $\text{PGL}_2(q)$. Let $a$ and $a^q$ be the two distinct roots of $f(x)$ in $\mathbb{F}_{q^2}$. Then \(\text{ord}(a) = q^2 - 1\), $a + a^q = -a$ and $a^{q+1} = b$. Put $P = \begin{pmatrix} 1 & 1 \\ a & a^q \end{pmatrix}$. Then $A_f$ can be diagonalized by the matrix $P$, i.e.,

$$P^{-1}A_fP = \begin{pmatrix} a & 0 \\ 0 & a^q \end{pmatrix}.$$

It is easy to check that $q + 1$ is the least positive integer $k$ such that $a^k = a^{q^k} = c$ for some $c \in \mathbb{F}_{q^a}$. Thus, \(\begin{pmatrix} a & 0 \\ 0 & a^q \end{pmatrix}\) has order $q + 1$ and hence $A_f$ generates a cyclic group of order $q + 1$ in $\text{PGL}_2(q)$.

Let $a_k = (a^{q^k} - a^k)/(a^q - a)$. Then the $k$-th power of $A_f$ can be calculated by

$$A_f^k = P \left( \begin{array}{c} a_k \\ 0 \end{array} \right) \cdot P^{-1} = \frac{1}{a^q - a} \left( a^{q^k + 1} - a^{q^k} \quad a^{q^k + 1} - a^{q^k} \right) = \left( \frac{-ba_k - 1}{a_k} \quad a_k \right).$$

Moreover, it is easy to verify that $a_k$ satisfies the following recursive formula

$$a_{k+2} + a_{k+1} + ba_k = 0 \quad \text{with} \quad a_0 = 0, \quad a_1 = 1.$$  

Let $\sigma$ be the automorphism of $\mathbb{F}_q(x)$ corresponding to the matrix $A_f$, i.e., $\sigma(x) = 1/(bx - a)$. Then we have

$$\sigma^k(x) = a_k,$$

It is easy to see that $a_k = 0$ if $\sigma^k = (a^{q^k} \leftrightarrow (q + 1)k)$. Thus, $a_k \neq 0$ for all $1 \leq k \leq q$. Hence, the order of $\sigma$ is $q + 1$.

Let $G$ be a subgroup of $\langle \sigma \rangle$. It is obviously that $\text{Tr}(x) = \sum_{\tau \in G} \tau(x)$ in $F^G$. By a direct computation, one has

$$\frac{a_{k+1}}{a_k} \neq \frac{a_{j+1}}{a_j}$$

for all $1 \leq k \neq j \leq q$. It follows that $\text{deg}(\text{Tr}(x)) = |G|$. By [19, Theorem 14.10], we have

$$|G| = [F : F^G] \leq [F : \mathbb{F}_q(\text{Tr}(x))] = \text{deg}(\text{Tr}(x)) = |G|.$$  

Hence, $F^G = F_q(\text{Tr}(x))$.

The ramification properties of $F/F^G$ are given in the following proposition and the number of rational places of $F$ in the extension $F/F^G$ can be completely determined.

**Proposition V.2.** Let $\sigma$ be an automorphism of $F$ of order $q + 1$ defined in Lemma VI.1. Let $G$ be a subgroup of $\langle \sigma \rangle$ of order $r + 1$ such that $(r + 1)(q + 1)$. Then the extension $F/F^G$ has the following properties:

(i) $[F : F^G] = r + 1$.

(ii) There is a unique place $Q$ of degree 2 of $F$ which is totally ramified in $F/F^G$ with ramification index $e_Q(F/F^G) = q + 1$ and different exponent $d_Q(F/F^G) = r$. There are exactly $(q + 1)/(r + 1)$ rational places of $F^G$ which split completely in $F/F^G$.

(iii) All other places of $F$ are unramified in $F/F^G$.

**Proof:** From Proposition II.3, there is a unique place $Q$ of degree 2 of $F$ which is totally ramified in $F/F^G$ with ramification index $e_Q(F/F^G) = q + 1$. Since $G$ is a subgroup of $\langle \sigma \rangle$, then $Q$ is totally ramified in $F/F^G$ with ramification index $e_Q(F/F^G) = r + 1$. It is easy to see that $r + 1$ is relatively prime to the characteristic of $\mathbb{F}_q$, i.e., $Q$ is tamely ramified in $F/F^G$. Hence, the different exponent of $Q$ is $d_Q(F/F^G) = e_Q(F/F^G) - 1 = r$.

From the Hurwitz genus formula, we have

$$2g(F) - 2 = |G| \cdot (2g(F^G) - 2) + \text{deg Diff}(F/F^G).$$

It follows that $\text{deg Diff}(F/F^G) = 2r = \text{deg}(r Q)$, i.e., $Q$ is the unique ramified place in $F/F^G$. The $q + 1$ rational places of $F$ are unramified in $F/F^G$. Furthermore, the relative degree of any rational place of $F$ is equal to one in $F/F^G$. Hence, there are exactly $(q + 1)/(r + 1)$ rational places of $F^G$ which split completely in $F/F^G$.

Now we can provide an explicit construction of optimal locally repairable codes with length $n = q + 1$ from subgroups of a cyclic subgroup of order $q + 1$ in $\text{Aut}(F/F_q)$.

**Theorem V.3.** Let $r$ be a positive integer such that $(r + 1)(q + 1)$. Put $n = m(r + 1)$ for any positive integer $m \leq \frac{q + 1}{r + 1}$. Then for any integer $t$ with $1 \leq t \leq m$, there exists an optimal $q$-ary $[n, k, d]$-locally repairable code with locality $r, k = rt$ and $d = n - k - \frac{k}{t} + 2$.

**Proof:** We prove the result only for $m = \frac{q + 1}{r + 1}$. This case gives the largest length $n = q + 1$. The reader may refer to Proposition III.1 for the proof of the case where $m < \frac{q + 1}{r + 1}$.

Let $F$ be the rational function field $F_q(x)$ and let $G$ be a subgroup of the cyclic group of order $q + 1$ defined in Lemma VI.1. In fact, there are exactly $m$ rational places $\{Q_1, \ldots, Q_m\}$ of $F^G$ which split completely in $F/F^G$ from Proposition V.2. Let $A_j = \{P_{j-1}((r+1)i+1), \ldots, P_{j+1}((r+1)i+1)\}$ be the set of rational places of $F$ lying over $Q_j$ for $1 \leq j \leq m$. Choose an element $z$ of $F^G$ such that $(z)^\infty = Q_1$. Then we must have $F^G = F_q(z)$. It is easy to see that $(z)^\infty = P_1 + \cdots + P_{r+1}$ in $F$, and $z$ is a constant function on each $A_j$ since $z(P_{j-1}((r+1)i+1)) = z(Q_j)$ for $1 \leq \ell \leq r+1, 1 \leq j \leq m$.

Choose an element $y$ in $F$ such that $(y)^\infty = P_{r+2}$ and $F = F_q(y)$. For $t > 1$, consider the set of functions

$$V := \left\{ \left( \sum_{i=0}^{r-1} \left( \sum_{j=0}^{t-1} a_{ij} z^j \right) y^j : a_{ij} \in \mathbb{F}_q \right) \right\}.$$

Let $G = (t-1)(z)^\infty + (r-1)(y)^\infty = (t-1)(P_1 + \cdots + P_{r+1}) + (r+1)P_{r+2}$. Then $V$ is a subspace of the Riemann-Roch space $\mathcal{L}(G)$.

Let $m_1 = v_{P_1}(G)$, then $m_1 = m_2 = \cdots = m_{r+1} = t - 1, m_{r+2} = r - 1$ and $m_{r+3} = \cdots = m_n = 0$. Put $\pi_1 = \cdots = \pi_{r+1} = 1/2$ and $\pi_{r+2} = 1/2$. Consider the subcode of the modified algebraic geometry code $C(P, V) = \{(\pi_1^{m_1} f)(P_1), \ldots, (\pi_{r+2}^{m_{r+2}} f)(P_{r+2}), f(P_{r+3}), \ldots, f(P_n) : f \in V\}$. It is easy to see that the code $C(P, V)$ is an $[n, k, d]$ code with $k = rt$ and $d = n - k - \frac{k}{t} + 2$.

It remains to prove that the code $C(P, V)$ has locality $r$. Denote by $(c_1, c_2, \ldots, c_n)$ the codeword

$$((\pi_1^{m_1} f)(P_1), \ldots, (\pi_{r+2}^{m_{r+2}} f)(P_{r+2}), f(P_{r+3}), \ldots, f(P_n))$$
for some \( f = \sum_{i=0}^{r-1} \left( \sum_{j=0}^{t-1} a_{ij} z^j \right) y^i \in V \) with \( a_{ij} \in \mathbb{F}_q \).

Suppose that the erased symbol of the codeword is \( c_\alpha = (\alpha^m f)(P_a) \), where \( P_a \in A_b \) with \( 1 \leq h \leq m \). For \( 3 \leq h \leq m \), the locality property follows from the proof of Proposition III.1. For \( h = 1 \), define the decoding polynomial

\[
\delta(y) = \sum_{i=0}^{r-1} \sum_{j=0}^{t-1} a_{ij} \pi_1^{-i} z^j (P_a) y^i = \sum_{i=0}^{r-1} a_{i,t-1} y^i.
\]

As we have shown in Proposition III.1, \( (\pi_1^{-i} f)(P_a) = \delta(y)(P_a) \) can be recovered from the other \( r \) symbols \( c_\beta = (\pi_1^{-i} f)(P_b) \) for \( P_b \in A_1 \setminus \{ P_a \} \) by the Lagrange interpolation. For \( h = 2 \), since \( \sum_{j=0}^{t-1} a_{ij} z^j \) is constant on \( A_2 \), we let \( b_1 = \sum_{j=0}^{t-1} a_{ij} z^j (P_{r+2}) \) for \( 0 \leq i \leq r - 2 \). Then we have \( (c_{r+2}, c_{r+3}, \ldots, c_{2r+2}) = (b_{r-1}, b_1, b_2, b_3, \ldots, b_{r} (P_2)) \).

**Case 1:** the erased symbol is \( c_{r+2} \) at \( P_{r+2} \). Since \( y(P_1) \) are pairwise distinct for \( r + 3 \leq \ell \leq 2r + 2 \), the coefficients \( b_1 \) for \( 0 \leq i \leq r - 1 \) can be determined by the Lagrange interpolation. Hence, the erased symbol \( c_{r+2} \) can be recovered.

**Case 2:** the erased symbol is \( c_w \) at \( P_w \) with \( r + 3 \leq w \leq 2r + 2 \). Then we have

\[
\sum_{i=0}^{r-2} b_i y^i (P_t) = c_t - b_{r-1} y^{-1} (P_t)
\]

for each \( \ell \) with \( r + 3 \leq \ell \neq w \leq 2r + 2 \). Hence, the coefficients \( b_0, \ldots, b_{r-2} \) can be determined by the Lagrange interpolation, i.e., the erased symbol \( c_w \) can also be recovered from \( c_\alpha = \sum_{i=0}^{r-1} b_i y^i (P_w) \).

**Example V.4.** For \( q = 11 \), we provide an explicit construction of an optimal [12, 2t, 14-t]-locally repairable code with locality 2 for each \( 1 \leq t \leq 4 \). First of all, we choose a quadratic primitive polynomial \( x^2 - 4x + 2 \in \mathbb{F}_{11}[x] \). Let \( \sigma \) be the automorphism of \( \mathbb{F}_{11}(x) \) which sends \( x \) to \( 1/(1-2x) \). Then the order of \( \sigma \) is 12. Let \( \omega_n \) be the numbers defined in the proof of Lemma V.1. Then we have \( \omega_2, \omega_3, \omega_{12}, \omega_{14}, \omega_{28} \) for \( 1 \leq t \leq 5 \). Let \( G = \langle \sigma^k \rangle \) be a subgroup of order 3. It follows that \( \sigma^\mu = \langle \mu \sigma \rangle \) (see [9, Theorem 11.91(iii)]).

**VI. Explicit Construction via Dihedral Subgroups**

Let \( F \) be the rational function field \( \mathbb{F}_q(x) \). In this section, we give an explicit construction of optimal locally repairable codes from a subgroup \( G \) of \( \text{Aut}(F/\mathbb{F}_q) \) that is isomorphic to some dihedral subgroup \( D_{2h} \) with \( h \geq 2 \). For odd \( q \), the order \( 2h \) of \( D_{2h} \) is a divisor of \( q - 1 \) or \( q + 1 \) by Theorem III.2. Thus, such localities \( r \) have already been obtained in Sections 4 and 5. Hence, we only consider even \( q \) in this section. From the Hurwitz genus formula, there are exactly 2+\( h \) rational places of \( F \) which are ramified in \( F/\mathbb{F}_q \) (see [9, Theorem 11.91(iii)]).

A. \( h \) Is a Divisor of \( q - 1 \)

In this subsection, \( h \geq 2 \) be a positive divisor of \( q - 1 \). Let \( \sigma \) be the automorphism of \( \mathbb{F}_q(x) \) determined by \( \sigma(x) = ax \) for \( a \in \mathbb{F}_q^* \) with \( \text{ord}(a) = h \), and let \( \tau \) be the automorphism of \( \mathbb{F}_q(x) \) determined by \( \tau(x) = 1/x \). Let \( G \) be the subgroup of \( \text{Aut}(F/\mathbb{F}_q) \) generated by \( \sigma \) and \( \tau \). Then it is easy to verify that \( G = \langle \sigma, \tau \rangle = \langle \sigma, \tau \sigma^h = 1, \tau \sigma^2 = 1, \tau \sigma = \tau^{-1} \rangle \supseteq D_{2h} \).

**Theorem VI.1.** Let \( h \geq 2 \) be a positive divisor of \( q - 1 \) for even \( q \). Put \( r = 2h - 1 \) and \( n = (r + 1)m \) for any positive integer \( m \leq \frac{q-1-h}{2h} \). Then for any integer \( t \) with \( 1 \leq t \leq m \), there exists an optimal \( n, k, d \), locally repairable code with locality \( r = rt \) and \( d = n - k - \frac{k}{r} + 2 \).

**Proof:** Let \( F \) be the rational function field \( \mathbb{F}_q(x) \). Let \( G = \langle \sigma, \tau \rangle \) be the subgroup of \( \text{Aut}(F/\mathbb{F}_q) \) of order
$r + 1 = 2h$ that is isomorphic to the dihedral subgroup $D_{2h}$, where $\sigma, \tau$ are defined as above. Let $P_\infty$ be the unique pole of $x$, i.e., $(x)_\infty = P_\infty$. It is easy to verify that $z = x^h + x^{-h}$ is an element of $F^G$. Moreover, the pole divisor of $z$ in $F$ is given by $(z)_\infty = hP_\infty + hP_0$. Hence, $F^G = \mathbb{F}_q(z)$. For $t \geq 1$, consider the set of functions

$$V := \left\{ \frac{1}{t-1} \left( \sum_{j=0}^{t-1} a_{ij} z^j \right) x^i : a_{ij} \in \mathbb{F}_q \right\}.$$

The rest of the proof is similar as that of Proposition III.1.

**Example VI.2.** Let $q = 16$ and $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ with $4 + \alpha + 1 = 1$. We give an explicit construction of an optimal $[12,5,14]$-locally repairable code with locality 5 for each $1 \leq t \leq 2$. Let $F$ be the rational function field $\mathbb{F}_{16}(x)$, let $\sigma(x) = \alpha^5 x$ be an automorphism of $\mathbb{F}_{16}(x)$ of order 3 and let $G = \langle \sigma, \tau \rangle$ be the dihedral subgroup $D_6$ of $\text{Aut}(F/\mathbb{F}_{16})$. It follows that $F^G = \mathbb{F}_{16}(z)$ where $z = x^3 + x^{-3}$. It is easy to verify that the infinity place $\infty$ of $F^G$ splits into two places $\{P_\infty, P_0\}$ in $F$ with ramification index 3, the zero of $z$ in $F^G$ splits into three places $\{P_1, P_a, P_{ap}\}$ of $F$ with ramification index 2, the zeros of $z - (\alpha^2 + \alpha + 1)$ and $z - (\alpha^2 + \alpha)$ of $F^G$ split completely in $F/\mathbb{F}_5$. In particular, $(z - \alpha^2 - \alpha - 1) = P_a + P_{a^2} + P_{a^3} + P_{a^4} + P_{a^5} + P_{a^6}$ and $(z - \alpha^2 - \alpha) = P_{a^2} + P_{a^3} + P_{a^4} + P_{a^5} + P_{a^6}$. Put

$$V := \left\{ \sum_{j=0}^{t-1} a_{ij} z^j x^i : a_{ij} \in \mathbb{F}_{16} \right\}.$$

Then the algebraic geometry code $C(P, V) = \{(f(P_a), f(P_{a^2}), f(P_{a^3}), f(P_{a^4}), f(P_{a^5}), f(P_{a^6}), f(P_{a^7}), f(P_{a^8}), f(P_{a^9}), f(P_{a^{10}})) : f \in V \}$ is an optimal $[12,5,14]$-locally repairable code with locality 5 for each $1 \leq t \leq 2$. Similar to Example VI.4, a generator matrix of such a code can be obtained as well. We skip the details.

**Example VI.3.** Let $q = 64$. Then

(i) by Theorem VI.1, there exists an optimal 64-ary $[60, 5t, 62 - 6t]$-locally repairable code with locality 5 for any $1 \leq t \leq 10$;

(ii) by Theorem VI.1, there exists an optimal 64-ary $[56, 13t, 58 - 14t]$-locally repairable code with locality 13 for any $1 \leq t \leq 4$;

(iii) by Theorem VI.1, there exists an optimal 64-ary $[54, 17t, 56 - 18t]$-locally repairable code with locality 17 for any $1 \leq t \leq 3$.

**B. h is a Divisor of q + 1**

Let $h \geq 2$ be a positive divisor of $q + 1$ in this subsection.

**Theorem VI.4.** Let $r$ be a positive integer such that $r + 1 = 2h$, where $h \geq 2$ is a positive divisor $q + 1$. Put $n = m(r + 1)$ for any positive integer $m \leq \frac{q - 1 - h}{r + 1}$. Then for any integer $t$ with $1 \leq t \leq m$, there exists an optimal $q$-ary $[n, k, d]$-locally repairable code with locality $r$, $k = rt$ and $d = n - k - \frac{k}{r} + 2$.

**Proof:** Let $F$ be the rational function field $\mathbb{F}_q(x)$ and let $P_\infty$ be the infinite place of $F$, i.e., $(x)_\infty = P_\infty$. Let $\sigma$ be the automorphism of $\mathbb{F}_q(x)$ of order $q + 1$ defined in Lemma V.1. Then $G := \langle \sigma^{\frac{q + 1}{h}}, \tau \rangle$ is isomorphic to the dihedral subgroup $D_{2h}$ of $\text{Aut}(F/\mathbb{F}_q)$, where $\tau$ is given by $\tau(x) = \frac{1}{x}$. Put

$$\mu(x) = \sum_{\rho \in G} \rho(x).$$

It is easy to verify that $z = \mu(x) \cdot \mu(x^{-1})$ is an element of $F^G$. Moreover, the degree of the pole divisor of $z$ in $F$ is $\deg(z)_\infty = 2h$. Hence, $F^G = \mathbb{F}_q(z)$. For $t \geq 1$, consider the set of functions

$$V := \left\{ \sum_{j=0}^{t-1} a_{ij} z^j x^i : a_{ij} \in \mathbb{F}_q \right\}.$$

Similarly, the proof can be completed by following that of Proposition III.1.

**Example VI.5.** Let $q = 64$. For each divisor $h \geq 2$ of 65, then

(i) by Theorem VI.4, there exists an optimal 64-ary $[50, 9t, 52 - 10t]$-locally repairable code with locality 9 for any $1 \leq t \leq 5$;

(ii) by Theorem VI.4, there exists an optimal 64-ary $[26, 5t, 2]$-locally repairable code with locality 25.

**VII. Conclusion**

In this paper, we show that as long as there is a subgroup $G$ of $\text{PGL}_2(q)$ of order $r + 1$, one can construct an optimal locally repairable code with locality $r$. These optimal locally repairable codes can be explicitly constructed as all subgroups of $\text{PGL}_2(q)$ have explicit structures. In this paper we provide explicit constructions of optimal locally repairable codes only for several subgroups such as affine subgroups, subgroups of a cyclic group of order $q + 1$ and dihedral subgroups. We also provide a general construction by estimating the number of ramified places regardless of subgroup structures.

It is clear that the construction given in this paper can be generalized to arbitrary function fields. We are currently working on the construction of locally repairable codes from maximal function fields and asymptotically optimal towers of function fields.

**References**

[1] A. Barg, K. Haymaker, E. W. Howe, G. L. Matthews, and A. Vardy-Alvarez, “Locally recoverable codes from algebraic curves and surfaces,” in *Algebraic Geometry for Coding Theory and Cryptography*, E. W. Howe, K. E. Lauter, and J. L. Walker, Eds. New York, NY, USA: Springer, 2017, pp. 95–127.

[2] A. Barg, I. Tamo, and S. Vlăduţ, “Locally recoverable codes on algebraic curves,” *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 4928–4939, Aug. 2017.

[3] V. R. Cadambe and A. Mazumdar, “Bounds on the size of locally recoverable codes,” *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 5778–5794, Nov. 2015.

[4] P. J. Cameron, G. R. Omidi, and B. Tayfeh-Rezaie, “3-Designs from PGL(2, q),” *Electron. J. Combinatorics*, vol. 13, no. 1, p. 50, 2006.

[5] L. E. Dickson, *Linear Groups: With an Exposition of the Galois Field Theory*. New York, NY, USA: Dover, 1958.

[6] M. Forbes and S. Yekhanin, “On the locality of codeword symbols in non-linear codes,” *Discrete Math.*, vol. 324, pp. 78–84, Jun. 2014.
[7] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, “On the locality of codeword symbols,” IEEE Trans. Inf. Theory, vol. 58, no. 11, pp. 6925–6934, Aug. 2012.

[8] J. Han and L. A. Lastras-Montano, “Reliable memories with subline accesses,” in Proc. IEEE Int. Symp. Inf. Theory, Jun. 2007, pp. 2531–2535.

[9] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, Algebraic Curves Over a Finite Field (Princeton Series in Applied Mathematics). Princeton, NJ, USA: Princeton Univ. Press, 2008.

[10] C. Huang, M. Chen, and J. Li, “Pyramid codes: Flexible schemes to trade space for access efficiency in reliable data storage systems,” in Proc. 6th IEEE Int. Symp. Netw. Comput. Appl., Jul. 2007, pp. 79–86.

[11] G. M. Kamath, N. Prakash, V. Lalitha, and P. V. Kumar, “Codes with local regeneration and erasure correction,” IEEE Trans. Inf. Theory, vol. 60, no. 8, pp. 4637–4660, Aug. 2014.

[12] D. Leemans and E. Schulte, “Polytopes with groups of type PGL2(q),” Ars Math. Contemporanea, vol. 2, no. 2, pp. 163–171, 2009.

[13] E. H. Moore, The Subgroups of the Generalized Finite Modular Group: The Decennial Publications, vol. 9. Chicago, IL, USA: Univ. of Chicago Press, 1904, pp. 141–190.

[14] H. Niederreiter and C. P. Xing, Rational Points on Curves Over Finite Fields: Theory and Applications (London Mathematical Society Lecture Note Series). Cambridge, U.K.: Cambridge Univ. Press, 2001, p. 285.

[15] D. S. Papailiopoulos and A. G. Dimakis, “Locally repairable codes,” IEEE Trans. Inf. Theory, vol. 60, no. 10, pp. 5843–5855, Oct. 2014.

[16] M. A. Tsfasman and S. Vlăduţ, Algebraic-Geometric Codes. Dordrecht, The Netherlands: Kluwer, 1993.

[17] M. A. Tsfasman, S. G. Vlăduţ, and D. Nogin, Algebraic Geometric Codes: Basic Notions. Providence, RI, USA: AMS, 1990.

[18] A. Wiman, “Bestimmung aller untergruppen einer doppelt unendlichen reihe von einfachen gruppen,” Bihandl Tll K. Svenska Vet.-Akad. Handl., vol. 25, pp. 1–47, 1899.

Lingfei Jin received her Ph.D degree in mathematics from Nanyang Technological University, Singapore in 2013. She is currently a Pre-tenure associate professor at the School of Computer Science, Fudan University, China. Her research interests include classical and quantum coding.

Liming Ma received his Ph.D. degree in Mathematics from Nanyang Technological University, Singapore in 2014. Since then he is a lecturer at the School of Mathematical Sciences, Yangzhou University, China. Dr. Ma is interested in algebraic function fields over finite fields and coding theory.

Chaoping Xing received his PhD degree in 1990 from University of Science and Technology of China. From 1990 to 1993 he was a lecturer and associate professor in the same university. He joined University of Essen, Germany as an Alexander von Humboldt fellow from 1993 to 1995. After this he spent most time in Institute of Information Processing, Austrian Academy of Sciences until 1998. From March of 1998 to November of 2007, he was working in National University of Singapore as an assistant/associate/full professor. Since December 2007, he has been with Nanyang Technological University as a full professor. Since November 2019, he has been with Shanghai Jiaotong University as a chair professor. Dr. Xing has been working on the areas of coding theory, cryptography, algebraic curves over finite fields and quasi-Monte Carlo methods, etc.