A new method for constructing linear codes with small hulls *

Liqin Qian, Xiwang Cao, Wei Lu, Patrick Solé

A new method for constructing linear codes with small hulls *

Liqin Qian†, Xiwang Cao‡, Wei Lu§, Patrick Solé¶

Abstract

The hull of a linear code over finite fields is the intersection of the code and its dual, which was introduced by Assmus and Key. In this paper, we develop a method to construct linear codes with trivial hull (LCD codes) and one-dimensional hull by employing the positive characteristic analogues of Gauss sums. These codes are quasi-abelian, and sometimes doubly circulant. Some sufficient conditions for a linear code to be an LCD code (resp. a linear code with one-dimensional hull) are presented. It is worth mentioning that we present a lower bound on the minimum distances of the constructed linear codes. As an application, using these conditions, we obtain some optimal or almost optimal LCD codes (resp. linear codes with one-dimensional hull) with respect to the online Database of Grassl.

Keywords: Linear codes, hull of a code, LCD codes, Gauss sums, quasi-abelian codes, double circulant codes
MSC(2010): 94B05, 11T24, 11T71

1 Introduction

The hull of a linear code C over a finite field is defined to be

$$\mathrm{Hull}(C) := C \cap C^{\perp}.$$

*This research is supported by the National Natural Science Foundation of China under Grant 11771007 and Grant 61572027.

†Liqin Qian, Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu, 210007, China, qianliqin_1108@163.com

‡Xiwang Cao, Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu, 210007, China; Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100042, China, xwcao@nuaa.edu.cn

§School of Mathematics, Southeast University, Nanjing, Jiangsu, 211189, China, luwei1010@seu.edu.cn

¶I2M(CNRS, Aix-Marseille University, Centrale Marseille), Marseilles, France, sole@enst.fr

It is clear that Hull(C) is also linear. It is easy to see that a linear code C is self-orthogonal if and only if the dimension of Hull(C) is the dimension of C, i.e., Hull(C) = C, and it is Linear Complementary Dual (LCD) if and only if the dimension of Hull(C) is zero, i.e., Hull(C) = $\{\mathbf{0}\}$. Specifically, a linear code C is self-dual if and only if the dimension of Hull(C) is $\frac{n}{2}$ for even n, where n is the length of C.

Hulls of linear codes have been introduced to classify finite projective planes in [1]. Later, it turned out that hulls of linear codes play a vital role in determining the complexity of some algorithms for checking permutation equivalence of two linear codes and computing the automorphism group of a linear code [12, 13, 22, 25]. It has been shown that these algorithms are always effective when the dimension of the hull is small. Due to their wide applications, some families of linear codes with special hulls such as LCD codes and linear codes with one-dimensional hull have been of interest and extensively studied [4, 14, 15, 16, 18, 23, 24]. It is worth noting that the equivalence of many types of codes with LCD codes has been extensively studied. Jin and Xing [10] showed that an algebraic geometry code over $\mathbb{F}_{2^m} (m \geq 7)$ is equivalent to an LCD code. Moreover, a celebrated result was presented in [5], which proved that any linear code over $\mathbb{F}_q$ $(q > 3)$ is equivalent to an LCD code. These codes are practically useful in communications systems, various applications, and link with other objects as shown in [3, 5, 6, 7, 9] and references therein. Consequently, it is of interest to study hulls, families of linear codes with small hulls. What needs to be emphasized is that Li and Zeng [18] constructed linear codes with one-dimensional hull by utilizing quadratic Gaussian sums from quadratic number fields and Carlet, Li and Mesnager [4] constructed LCD codes and linear codes with one-dimensional hull by employing character sums in semi-primitive case from cyclotomic fields and multiplicative subgroups of finite fields. They have made a lot of contributions in this regard.

Inspired by the above research work, we construct LCD codes and codes with one-dimensional hull dimension, by using an analogue of Gauss sums where both the corresponding additive and multiplicative character take their take values in a finite field instead of the complex numbers. This method generalizes previous work [18, 20, 21]. Moreover, we consider the order $N \geq 2$ of the homomorphism, while [18] only considers $N = 2$. It turns out that our constructions are more general and direct than previous work on small hulls of linear codes. It is worth observing that we obtain some optimal or almost optimal LCD codes and linear codes with one-dimensional hull from our constructions. Compared with [18], the linear codes we constructed may be new when $N > 2$ in the sense. Furthermore, we also present a lower bound on the minimum distances of the codes presented in this paper. These codes have a lot of built-in symmetry: they are quasi-abelian of index 2 in general [11], and double circulant in many cases.

The rest of this paper is organized as follows. Section 2 gives the preliminaries. In

Section 3, we give two concrete homomorphisms from a finite field into a finite field and present the idea of constructing linear codes determined by a special generator matrix. In Sections 4 and 5, we investigate LCD codes and linear codes with one-dimensional hull by employing these two homomorphisms from a finite field to a finite field, respectively. In addition, we present some examples of optimal or almost optimal LCD codes and linear codes with one-dimensional hull. In Section 6, we present a lower bound on the minimum distances of the constructed linear codes. Section 7 concludes the article.

2 Preliminaries

In this section, we introduce some notation and results in order for the exposition in this paper to be self-contained, which will be useful later.

2.1 Codes

Let q be a power of a prime p and $\mathbb{F}_q$ denote the finite field with q elements. For a positive integer n, a linear code of length n over $\mathbb{F}_q$ is defined to be a subspace of the $\mathbb{F}_q$-vector spaces $\mathbb{F}_q^n$. A linear code C of length n over $\mathbb{F}_q$ is called an $[n,k,d]_q$ code if its $\mathbb{F}_q$-dimension is k and the minimum Hamming distance of C is d. If C is an $[n,k,d]$ code, then from the Singleton bound, its minimum distance is bounded above by $d \leq n-k+1$. A code meeting the above bound is called Maximum Distance Separable (MDS). A code is called almost MDS if its minimum distance is one less than the MDS case. For $\boldsymbol{u} := (u_1, u_2, \cdots, u_n)$ and $\boldsymbol{v} := (v_1, v_2, \cdots, v_n)$ in $\mathbb{F}_q^n$, the inner product of $\boldsymbol{u}$ and $\boldsymbol{v}$ is defined to be $\langle \boldsymbol{u}, \boldsymbol{v} \rangle := \sum_{i=1}^{n} u_i v_i$. The dual $C^\perp$ of a linear code C of length n over $\mathbb{F}_q$ is defined to be the set $C^\perp = \{\boldsymbol{v} \in \mathbb{F}_q^n | \langle \boldsymbol{c}, \boldsymbol{v} \rangle = 0 \text{ for all } \boldsymbol{c} \in C\}$. A linear code C is said to be self-orthogonal if $C \subseteq C^\perp$ and it is said to be self-dual if $C = C^\perp$. A linear code C is said to be linear complementary dual (LCD) code if $C \cap C^\perp = \{0\}$.

2.2 Homomorphisms

Starting from this subsection till the end of this paper, we let $\mathbb{F}_{r^m}$ denote the finite field of order r^m, where r is a prime number and m is a positive integer. Let $\mathbb{F}_{r^m}^* = \mathbb{F}_{r^m} \backslash \{0\}$. Let $\overline{\mathbb{F}}_q$ be the algebraic closure of the finite field $\mathbb{F}_q$.

Let φ be a homomorphism from $\mathbb{F}_{r^m}^*$ into $\overline{\mathbb{F}}_q^*$, that is, a mapping from $\mathbb{F}_{r^m}^*$ into $\overline{\mathbb{F}}_q^*$ with $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in \mathbb{F}_{r^m}^*$. Define $\overline{\varphi}(x) := \varphi(x^{-1})$. Let φ_0 be the trivial homomorphism, which is defined by $\varphi_0(x) = 1$ for all $x \in \mathbb{F}_{r^m}^*$.

The following lemma gives the orthogonality relations of the homomorphism φ.

Lemma 2.1. *Let φ be defined as above. Then we have*

$$\sum_{x\in\mathbb{F}_{r^m}^*}\varphi(x)=\begin{cases} r^m-1, & \text{if } \varphi=\varphi_0;\\ 0, & \text{if } \varphi\neq\varphi_0.\end{cases}$$

Proof. The proof is similar to that of [17, Theorem 5.4] and omitted here. □

Let χ be a homomorphism from $\mathbb{F}_{r^m}$ into $\overline{\mathbb{F}}_q^*$, that is, a mapping from $\mathbb{F}_{r^m}$ into $\overline{\mathbb{F}}_q^*$ with $\chi(x+y)=\chi(x)\chi(y)$ for all $x,y\in\mathbb{F}_{r^m}$. Define $\overline{\chi}(x):=\chi(-x)$. Let χ_0 be the trivial homomorphism, which is defined by $\chi_0(x)=1$ for all $x\in\mathbb{F}_{r^m}$.

We also have the following lemma, which presents the orthogonality relations of the homomorphism χ.

Lemma 2.2. *Let χ be defined as above. Then we have*

$$\sum_{x\in\mathbb{F}_{r^m}}\chi(x)=\begin{cases} r^m, & \text{if } \chi=\chi_0;\\ 0, & \text{if } \chi\neq\chi_0.\end{cases}$$

Proof. The proof is similar to that of [17, Theorem 5.4] and omitted here. □

2.3 Some results for the sum $g(\varphi,\chi)$

Let φ and χ be defined as Subsection 2.1. Then we define the sums

$$g(\varphi,\chi)=\sum_{x\in\mathbb{F}_{r^m}^*}\varphi(x)\chi(x)$$

and

$$\overline{g(\varphi,\chi)}=g(\overline{\varphi},\overline{\chi})=\sum_{x\in\mathbb{F}_{r^m}^*}\varphi(x^{-1})\chi(-x).$$

The following results show the value of the sum $g(\varphi,\chi)$.

Lemma 2.3. *Let φ and χ be defined as Subsection 2.1. Then the sum $g(\varphi,\chi)$ satisfies*

$$g(\varphi,\chi)=\begin{cases} r^m-1, & \text{if } \varphi=\varphi_0 \text{ and } \chi=\chi_0;\\ -1, & \text{if } \varphi=\varphi_0 \text{ and } \chi\neq\chi_0;\\ 0, & \text{if } \varphi\neq\varphi_0 \text{ and } \chi=\chi_0.\end{cases}$$

Proof. The conclusion follows directly from Lemmas 2.1 and 2.2. □

Lemma 2.4. *Let φ and χ be defined as Subsection 2.1. If $\varphi\neq\varphi_0$ and $\chi\neq\chi_0$, then*

$$g(\varphi,\chi)\overline{g(\varphi,\chi)}=r^m\in\mathbb{F}_p.$$

Proof. For $\varphi \neq \varphi_0$ and $\chi \neq \chi_0$, we get

$$\begin{aligned}
g(\varphi,\chi)\overline{g(\varphi,\chi)} &= \sum_{x\in\mathbb{F}_{r^m}^*}\varphi(x)\chi(x)\sum_{y\in\mathbb{F}_{r^m}^*}\varphi(y^{-1})\chi(-y)\\
&= \sum_{x,y\in\mathbb{F}_{r^m}^*}\varphi(xy^{-1})\chi(x-y)\\
x\longrightarrow xy \quad &\sum_{x,y\in\mathbb{F}_{r^m}^*}\varphi(x)\chi(y(x-1))\\
&= \sum_{x\in\mathbb{F}_{r^m}^*}\varphi(x)\sum_{y\in\mathbb{F}_{r^m}^*}\chi(y(x-1))\\
&= \varphi(1)\sum_{y\in\mathbb{F}_{r^m}^*}\chi(0)+\sum_{x\in\mathbb{F}_{r^m}^*\setminus\{1\}}\varphi(x)\sum_{y\in\mathbb{F}_{r^m}^*}\chi(y(x-1))\\
&= r^m-1-\sum_{x\in\mathbb{F}_{r^m}^*\setminus\{1\}}\varphi(x)\\
&= r^m-\sum_{x\in\mathbb{F}_{r^m}^*}\varphi(x)\\
&= r^m.
\end{aligned}$$

This completes the proof of this lemma. □

The study of the behavior of the sum $g(\varphi,\chi)$ under various transformations of the φ or χ leads to a number of useful identities.

Lemma 2.5. *Let φ and χ be defined as Subsection 2.1. Then we have the following results.*

(1) $g(\varphi,\overline{\chi}) = \varphi(-1)g(\varphi,\chi)$;

(2) $g(\overline{\varphi},\chi) = \varphi(-1)\overline{g(\varphi,\chi)}$;

(3) $g(\varphi,\chi)g(\overline{\varphi},\chi) = \varphi(-1)r^m$ *for* $\varphi\neq\varphi_0$ *and* $\chi\neq\chi_0$;

(4) $(g(\varphi,\chi))^{p^s} = g(\varphi^{p^s},\chi^{p^s})$, *where p is the characteristic of $\mathbb{F}_q$ and s is a positive integer.*

Proof. The results of (1)-(3) are obvious by the definition $g(\varphi,\chi)$ and Lemma 2.4. Next, we prove the result of (4). Combined with the definitions of φ and χ, we have

$$(g(\varphi,\chi))^{p^s} = \left(\sum_{x\in\mathbb{F}_{r^m}^*}\varphi(x)\chi(x)\right)^{p^s} = \sum_{x\in\mathbb{F}_{r^m}^*}(\varphi(x))^{p^s}(\chi(x))^{p^s} = \sum_{x\in\mathbb{F}_{r^m}^*}\varphi^{p^s}(x)\chi^{p^s}(x) = g(\varphi^{p^s},\chi^{p^s}).$$

□

Remark 2.6. *The φ and χ in Section 2.1 are not the usual multiplicative and additive characters, respectively. Moreover, the $g(\varphi,\chi)$ is also not the usual Gaussian sums. However,*

we can prove that the sum $g(\varphi, \chi)$ has similar properties to Gaussian sums (see Lemmas 2.3 and 2.5(1-3)). The definition of the sum $g(\varphi, \chi)$ may have been studied before, but we haven't found any relevant references.

2.4 On characterizations of LCD codes and codes having one-dimensional hull

In this paper, we consider the constructions of linear codes with small hull, mainly refer to LCD codes and linear codes with one-dimensional hull. We will characterize when a linear code is an LCD code or a linear code with one-dimensional hull. We next present two lemmas for this purpose.

A complete characterization of LCD codes via the nonsingularity of their generator matrices was employed in [3, 19], which provides a sufficient and necessary condition for a linear code to be an LCD code.

Lemma 2.7. *[3, 19] Let C be an $[n, k]$ linear code over $\mathbb{F}_q$ with generator matrix $G = [I_k, P]$. Then the code C is LCD if and only if $I_k + PP^T$ is nonsingular, i.e., -1 is not an eigenvalue of the matrix PP^T, where P^T denotes the transpose of P.*

We also have the following lemma on a linear code having one-dimensional hull, which provides an idea to construct linear codes with one-dimensional hull by using the eigenvalues of the generator matrices.

Lemma 2.8. *[4, 18] Let C be an $[n, k]$ linear code over $\mathbb{F}_q$ with generator matrix $G = [I_k, P]$. Then the code C has one-dimensional hull if the matrix PP^T has an eigenvalue -1 with (algebraic) multiplicity 1.*

3 Linear codes associated with homomorphisms

In this section, we construct the linear codes by using the two homomorphisms in Section 2.1.

Let r be a prime number and m a positive integer. $\mathbb{F}_{r^m}$ denotes the finite field of order r^m. Let $\mathbb{F}_{r^m}^* = \mathbb{F}_{r^m} \backslash \{0\}$ and $\mathbb{F}_{r^m}^* = \langle \alpha \rangle$, where α is a fixed primitive element of $\mathbb{F}_{r^m}^*$. Assume that $N > 1$ is a positive integer and $N | (r^m - 1)$. Let q be a power of p, where p is a prime number. Assume that $N | (q - 1)$. Let $\mathbb{F}_q^* = \langle \beta \rangle$, where β is a fixed primitive element of $\mathbb{F}_q^*$. For the sake of convenience, we let $u = \beta^{\frac{q-1}{N}}$. Define the function

$$\varphi : \mathbb{F}_{r^m}^* \longrightarrow \mathbb{F}_q^*, \varphi(\alpha^k) = u^k, \tag{1}$$

where $0 \leq k \leq r^m - 2$. It is easy to know that φ is a homomorphism of order N. Define the kernel of the homomorphism φ is the set

$$\ker(\varphi) := \{\alpha^k, 0 \leq k \leq r^m - 2 : \varphi(\alpha^k) = 1\} = \langle \alpha^N \rangle.$$

Assume that $(p, r) = 1$. Then there exists a positive integer t such that $r|(q^t - 1)$. Let $\mathbb{F}_{q^t}^* = \langle \gamma \rangle$ and $\zeta = \gamma^{\frac{q^t-1}{r}}$, where γ is a fixed primitive element of $\mathbb{F}_{q^t}^*$. For any $a \in \mathbb{F}_{r^m}$, we define

$$\chi_a : \mathbb{F}_{r^m} \longrightarrow \overline{\mathbb{F}}_q^*, \chi_a(x) = \zeta^{\mathrm{Tr}_r^{r^m}(ax)}, x \in \mathbb{F}_{r^m}, \tag{2}$$

where $\mathrm{Tr}_r^{r^m}$ denotes the trace function from $\mathbb{F}_{r^m}$ onto $\mathbb{F}_r$. It is easy to know that χ_a is a homomorphism. It follows from the definition of χ_a that

$$g(\varphi, \chi_{ab}) \quad = \quad \overline{\varphi}(b) g(\varphi, \chi_a) \tag{3}$$

for $a \in \mathbb{F}_{r^m}$ and $b \in \mathbb{F}_{r^m}^*$.

Fix $v \in \mathbb{F}_q$. Let $\mathbb{F}_{r^m} = \{x_i : 1 \leq i \leq r^m\}$. Define the $r^m \times r^m$ matrix $P = (p_{ij}) \in M_{r^m}(\mathbb{F}_q)$ by $p_{ij} = \rho(x_j - x_i)$, where

$$\rho(x_j - x_i) = \begin{cases} \varphi(x_j - x_i), & \text{if } i \neq j; \\ v, & \text{if } i = j. \end{cases} \tag{4}$$

For any $a \in \mathbb{F}_{r^m}$, set $\eta_a := (\chi_a(x_1), \chi_a(x_2), \cdots, \chi_a(x_{r^m}))^T$, where "$T$" denotes the transpose operator. Then the ith component of $P\eta_a$ is

$$\sum_{j=1}^{r^m} \rho(x_j - x_i)\chi_a(x_j) = \sum_{x \in \mathbb{F}_{r^m}} \rho(x - x_i)\chi_a(x) y := x - x_i \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(y + x_i) = \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(y)\chi_a(x_i).$$

Hence, $P\eta_a = \left(\sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(y) \right) \eta_a$ and η_a is an eigenvector of P.

Similarly, the ith component of $P^T\eta_a$ is

$$\sum_{j=1}^{r^m} \rho(x_i - x_j)\chi_a(x_j) = \sum_{x \in \mathbb{F}_{r^m}} \rho(x_i - x)\chi(x) y := x_i - x \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(x_i - y) = \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(-y)\chi_a(x_i).$$

Hence, $P^T\eta_a = \left(\sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(-y) \right) \eta_a$ and η_a is also an eigenvector of P^T.

Next, we will prove that the r^m vectors $\{\eta_a := (\chi_a(x_1), \chi_a(x_2), \cdots, \chi_a(x_{r^m}))^T : a \in \mathbb{F}_{r^m}\}$ are linearly independent over $\overline{\mathbb{F}}_q$.

Suppose that $\sum_{a\in\mathbb{F}_{r^m}} k_a\eta_a = \mathbf{0}$, where $k_a \in \overline{\mathbb{F}}_q$. Then we have

$$\begin{aligned}
&\sum_{a\in\mathbb{F}_{r^m}} k_a(\chi_a(x_1), \chi_a(x_2), \cdots, \chi_a(x_{r^m}))^T = \mathbf{0},\\
\Longrightarrow\quad &\left(\sum_{a\in\mathbb{F}_{r^m}} k_a\chi_a(x_1), \sum_{a\in\mathbb{F}_{r^m}} k_a\chi_a(x_2), \cdots, \sum_{a\in\mathbb{F}_{r^m}} k_a\chi_a(x_{r^m})\right)^T = \mathbf{0}.
\end{aligned}$$

Hence, $\sum_{a\in\mathbb{F}_{r^m}} k_a\chi_a(x_i) = 0$ for any $1 \le i \le r^m$.

Given an element $a_0 \in \mathbb{F}_{r^m}$, we have

$$\begin{aligned}
&\sum_{a\in\mathbb{F}_{r^m}} k_a\chi_a(x_i)\chi_{a_0}(-x_i) = 0 \text{ for any } 1 \le i \le r^m,\\
\Longrightarrow\quad &\sum_{a\in\mathbb{F}_{r^m}} k_a\chi_1((a-a_0)x_i) = 0 \text{ for any } 1 \le i \le r^m,\\
\Longrightarrow\quad &\sum_{x\in\mathbb{F}_{r^m}}\sum_{a\in\mathbb{F}_{r^m}} k_a\chi_1((a-a_0)x) = 0,\\
\Longrightarrow\quad &\sum_{a\in\mathbb{F}_{r^m}} k_a \sum_{x\in\mathbb{F}_{r^m}} \chi_1((a-a_0)x) = 0.
\end{aligned}$$

By Lemma 2.2, we obtain $k_{a_0}r^m = 0$ and then $k_{a_0} = 0$ by $(r, p) = 1$. Because a_0 is arbitrary, we have $k_a = 0$ for any $a \in \mathbb{F}_{r^m}$. Hence, the r^m vectors $\{\eta_a := (\chi_a(x_1), \chi_a(x_2), \cdots, \chi_a(x_{r^m}))^T : a \in \mathbb{F}_{r^m}\}$ are linearly independent over $\overline{\mathbb{F}}_q$.

Therefore, the multisets $\left\{\sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(y) : a \in \mathbb{F}_{r^m}\right\}$ and $\left\{\sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(-y) : a \in \mathbb{F}_{r^m}\right\}$ present all eigenvalues of the matrix P and P^T, respectively.

To sum up, $PP^T\eta_a = P\left(\sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(-y)\right)\eta_a = \left(\sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(y)\sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(-y)\right)\eta_a$. Then the multiset $\left\{\lambda_a := \sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(y)\sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(-y) : a \in \mathbb{F}_{r^m}\right\}$ presents all eigenvalues of the matrix PP^T and $\{\eta_a : a \in \mathbb{F}_{r^m}\}$ presents all eigenvectors of PP^T.

Let the symbols be the same as above. According to Lemma 2.5(1), we obtain

$$\begin{aligned}
\lambda_a &= \sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(y) \sum_{y\in\mathbb{F}_{r^m}} \rho(y)\chi_a(-y) \\
&= \left(v + \sum_{y\in\mathbb{F}_{r^m}^*} \varphi(y)\chi_a(y)\right)\left(v + \sum_{y\in\mathbb{F}_{r^m}^*} \varphi(y)\chi_a(-y)\right) \\
&= (v + g(\varphi,\chi_a))(v + g(\varphi,\overline{\chi}_a)) \\
&= v^2 + vg(\varphi,\chi_a) + vg(\varphi,\overline{\chi}_a) + g(\varphi,\chi_a)g(\varphi,\overline{\chi}_a) \\
&= v^2 + vg(\varphi,\chi_a) + \varphi(-1)vg(\varphi,\chi_a) + \varphi(-1)(g(\varphi,\chi_a))^2 \\
&= v^2 + (1+\varphi(-1))vg(\varphi,\chi_a) + \varphi(-1)(g(\varphi,\chi_a))^2.
\end{aligned}$$

Hence, all eigenvalues of PP^T are given by the multiset

$$\{\lambda_a := v^2 + (1+\varphi(-1))vg(\varphi,\chi_a) + \varphi(-1)(g(\varphi,\chi_a))^2 : a \in \mathbb{F}_{r^m}\}. \tag{5}$$

Let $C := C_{(\varphi,v)}$ be a linear code over $\mathbb{F}_q$ with generator matrix $G = [I_{r^m}, P]$. Then C is a $[2r^m, r^m]$ linear code over $\mathbb{F}_q$. In Section 4, we construct LCD codes according to Lemma 2.7. In Section 5, we construct linear codes with one-dimensional hull by Lemma 2.8.

4 The constructions of LCD codes

In this section, we present two simple constructions of LCD codes by using the two homomorphisms (1) and (2). When $m = 1$ these codes are double circulant. In general, they are quasi-abelian of index 2 as $\mathbb{F}_q[H]-$submodules of $\mathbb{F}_q[H]^2$ with H the additive group of $\mathbb{F}_{r^m}$ [11].

Construction A. *Define $\rho(0) = v = 0$. We then obtain a $r^m \times r^m$ matrix $P = (p_{ij})$ by*

$$p_{ij} = \rho(x_j - x_i),$$

which is defined as (4). It follows from (5) that all eigenvalues of PP^T are given by

$$\lambda_a = \begin{cases} 0, & \text{if } a = 0; \\ \varphi(-1)(g(\varphi,\chi_a))^2, & \text{if } a \in \mathbb{F}_{r^m}^*. \end{cases} \tag{6}$$

The following theorem gives the sufficient conditions for linear codes to be LCD codes by Construction A.

Theorem 4.1. *Let r be a prime number and m be a positive integer. Assume that $N > 1$ is a positive integer and $N|(r^m - 1)$. Let q be a power of prime p and $(p, r) = 1$. Assume that $N|(q-1)$. Let $C := C_{(\varphi,0)}$ be the linear code over $\mathbb{F}_q$ with generator matrix $[I_{r^m}, P]$. Then we have the following.*

(1) If there exists a positive integer s such that $N|(p^s-1)$ and $\varphi(p^{2s}) \neq 1$, then C is a $[2r^m, r^m]$ LCD code over $\mathbb{F}_q$. In particular, if $\varphi(q^2) \neq 1$, then C is an $[2r^m, r^m]$ LCD code over $\mathbb{F}_q$.

(2) If there exists a positive integer s such that $N|(p^s+1)$ and $\varphi(p^{-2s}) \neq r^{2m}$, then C is an $[2r^m, r^m]$ LCD code over $\mathbb{F}_q$.

Proof. It follows from (6) that all eigenvalues of PP^T are 0 when $a = 0$ and $\varphi(-1)(g(\varphi, \chi_a))^2$ when $a \in \mathbb{F}_{r^m}^*$. According to Lemma 2.7, we just have to prove that $\varphi(-1)(g(\varphi, \chi_a))^2 \neq -1$ for any $a \in \mathbb{F}_{r^m}^*$. Assume on the contrary that there exists $a \in \mathbb{F}_{r^m}^*$ such that $\varphi(-1)(g(\varphi, \chi_a))^2 = -1$.

(1) If there exists a positive integer s such that $N|(p^s-1)$, we get $\varphi^{p^s} = \varphi$. Then

$$\begin{aligned}
& (\varphi(-1)(g(\varphi, \chi_a))^2)^{p^s} = (-1)^{p^s} = -1 \\
\Longrightarrow \quad & (\varphi(-1))^{p^s}(g(\varphi, \chi_a))^{p^s})^2 = -1 \\
\Longrightarrow \quad & \varphi^{p^s}(-1)(g(\varphi^{p^s}, \chi_{ap^s}))^2 = -1 \\
\Longrightarrow \quad & \varphi(-1)(g(\varphi, \chi_{ap^s}))^2 = -1 \\
\Longrightarrow \quad & \varphi(-1)(\overline{\varphi}(p^s)g(\varphi, \chi_a))^2 = -1 \\
\Longrightarrow \quad & \varphi(-1)(g(\varphi, \chi_a))^2 = -(\overline{\varphi}(p^s))^{-2} = -\varphi(p^{2s}).
\end{aligned}$$

Combined $\varphi(-1)(g(\varphi, \chi_a))^2 = -1$ with $\varphi(-1)(g(\varphi, \chi_a))^2 = -\varphi(p^{2s})$, we get $\varphi(p^{2s}) = 1$ which is a contradiction. Hence, $\varphi(-1)(g(\varphi, \chi_a))^2 \neq -1$ for any $a \in \mathbb{F}_{r^m}^*$.

(2) If there exists a positive integer s such that $N|(p^s+1)$, we get $\varphi^{p^s} = \varphi^{-1}$. Then

$$\begin{aligned}
& (\varphi(-1)(g(\varphi, \chi_a))^2)^{p^s} = (-1)^{p^s} = -1 \\
\Longrightarrow \quad & \varphi^{p^s}(-1)(g(\varphi^{p^s}, \chi_{ap^s}))^2 = -1 \\
\Longrightarrow \quad & \varphi^{-1}(-1)(g(\varphi^{-1}, \chi_{ap^s}))^2 = -1 \\
\Longrightarrow \quad & \varphi^{-1}(-1)(\overline{\varphi^{-1}}(p^s)\overline{\varphi^{-1}}(-1)g(\varphi^{-1}, \chi_{-a}))^2 = -1 \\
\Longrightarrow \quad & \varphi^{-1}(-1)(g(\varphi^{-1}, \chi_{-a}))^2 = -(\varphi^{-1}(p^{-s})\varphi^{-1}(-1))^{-2} = -\varphi(p^{-2s}) \\
\Longrightarrow \quad & \varphi^{-1}(-1)(\overline{g(\varphi, \chi_a)})^2 = -\varphi(p^{-2s}).
\end{aligned}$$

Combined $\varphi(-1)(g(\varphi, \chi_a))^2 = -1$ with $\varphi^{-1}(-1)(\overline{g(\varphi, \chi_a)})^2 = -\varphi(p^{-2s})$, we get

$$\begin{aligned}
& \varphi(-1)(g(\varphi, \chi_a))^2\varphi^{-1}(-1)(\overline{g(\varphi, \chi_a)})^2 = \varphi(p^{-2s}) \\
\Longrightarrow \quad & (g(\varphi, \chi_a)\overline{g(\varphi, \chi_a)})^2 = \varphi(p^{-2s}) \\
\Longrightarrow \quad & r^{2m} = \varphi(p^{-2s}) \text{ by Lemma 2.4,}
\end{aligned}$$

which is a contradiction. Therefore, $\varphi(-1)(g(\varphi, \chi_a))^2 \neq -1$ for any $a \in \mathbb{F}_{r^m}^*$.

To sum up, -1 is not an eigenvalue of the matrix PP^T. By Lemma 2.7, C is an $[2r^m, r^m]$ LCD code over $\mathbb{F}_q$. This finishes the proof of the theorem. □

Two concrete examples with respect to Theorem 4.1 are given as follows.

Example 4.2. *Let $r = 7, m = 1, N = 3, p = 2$ and $q = 4$. Let $\mathbb{F}_4^* = \langle\beta\rangle$, where β is a fixed primitive element of $\mathbb{F}_4^*$. It is easy to check that q, r, N satisfy the conditions in Theorem 4.1(1)(2). Then C is a quaternary $[14, 7, 5]$ LCD code with generator matrix $[I_7, P]$, where*

$$P = \begin{pmatrix} 0 & 1 & \beta^2 & \beta & \beta & \beta^2 & 1 \\ 1 & 0 & 1 & \beta^2 & \beta & \beta & \beta^2 \\ \beta^2 & 1 & 0 & 1 & \beta^2 & \beta & \beta \\ \beta & \beta^2 & 1 & 0 & 1 & \beta^2 & \beta \\ \beta & \beta & \beta^2 & 1 & 0 & 1 & \beta^2 \\ \beta^2 & \beta & \beta & \beta^2 & 1 & 0 & 1 \\ 1 & \beta^2 & \beta & \beta & \beta^2 & 1 & 0 \end{pmatrix},$$

which is almost optimal in the sense that the minimum distance of the optimal quaternary linear code with the length 14 and the dimension 7 is 6 by the online Database [8]. Moreover, the dual code of C has parameters $[14, 7, 5]$, which is also almost optimal.

Example 4.3. *Let $r = 3, m = 1, N = 2$ and $q = p = 5$. It is easy to check that q, r, N satisfy the conditions in Theorem 4.1(2). Then C is an $[6, 3, 3]$ LCD code over $\mathbb{F}_5$ with generator matrix $[I_3, P]$, where*

$$P = \begin{pmatrix} 0 & 1 & -1 \\ -1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix},$$

which is almost optimal in the sense that the minimum distance of the optimal 5-ary linear code with the length 6 and the dimension 3 is 4 by the online Database [8]. Moreover, the dual code of C has parameters $[6, 3, 3]$, which is also almost optimal.

In view of Theorem 4.1, since the sufficient condition is abstract for a linear code to be an LCD code, we present a concrete result as corollary in the following.

Corollary 4.4. *Let r be a prime number and m be a positive integer. Assume that $N > 1$ is a positive integer and $N|(r^m - 1)$. Let q be a power of prime p and $(p, r) = 1$. Assume that $N|(q - 1)$. Let $C := C_{(\varphi,0)}$ be the linear code over $\mathbb{F}_q$ with generator matrix $[I_{r^m}, P]$. Then we have the following.*

(1) If there exists a positive integer s such that $N|(p^s - 1)$ and $p^{\frac{2s(r^m-1)}{N}} \not\equiv 1 \pmod{r}$, then C is an $[2r^m, r^m]$ LCD code over $\mathbb{F}_q$.

(2) If there exists a positive integer s such that $N|(p^s+1)$ and $r^{2mN} \not\equiv 1 \pmod{p}$, then C is an $[2r^m, r^m]$ LCD code over $\mathbb{F}_q$.

Proof. Compared with the conditions of Theorem 4.1, we just have to prove that (1) if $p^{\frac{2s(r^m-1)}{N}} \not\equiv 1 \pmod{r}$, then $\varphi(p^{2s}) \neq 1$ and (2) if $r^{2mN} \not\equiv 1 \pmod{p}$, then $\varphi(p^{-2s}) \neq r^{2m}$, respectively.

(1) Assume on the contrary that $\varphi(p^{2s}) = 1$, then $p^{2s} \in \ker(\varphi)$. Hence, $p^{2s} \in \langle \alpha^N \rangle$. Since $\mathrm{ord}(\alpha^N) = \frac{r^m-1}{N}$, we have $p^{2s \cdot \frac{r^m-1}{N}} \equiv 1 \pmod{r}$, it is a contradiction.

(2) Assume on the contrary that $\varphi(p^{-2s}) = r^{2m}$, then $(\varphi(p^{-2s}))^N = r^{2mN}$. Hence, $r^{2mN} \equiv 1 \pmod{p}$, it is a contradiction. This completes the proof. □

Construction B. *Define $\rho(0) = v$. We then obtain a $r^m \times r^m$ matrix $P = (p_{ij})$ by*

$$p_{ij} = \rho(x_j - x_i),$$

which is defined as (4). For any $a \in \mathbb{F}_{r^m}$, we define $f_a : \mathbb{F}_q \longrightarrow \overline{\mathbb{F}}_q$ by

$$f_a(x) = \begin{cases} x^2, & \text{if } a = 0; \\ x^2 + (1+\varphi(-1))\overline{\varphi}(a)g(\varphi,\chi_1)x + \varphi(-1)(\overline{\varphi}(a)g(\varphi,\chi_1))^2, & \text{if } a \in \mathbb{F}_{r^m}^*. \end{cases} \tag{7}$$

It follows from (5) that all eigenvalues of PP^T are given by

$$\lambda_a := f_a(v)$$

for all $a \in \mathbb{F}_{r^m}$.

In order to construct LCD codes over $\mathbb{F}_q$, we hope that there exists $v \in \mathbb{F}_q$ satisfying $f_a(v) \neq -1$ for any $a \in \mathbb{F}_{r^m}$. Hence, we present a lemma as follows.

Lemma 4.5. *Let the symbols be the same as above. If $q > 2(N+1)$, then there exists $v \in \mathbb{F}_q$ satisfying $\lambda_a := f_a(v) \neq -1$ for any $a \in \mathbb{F}_{r^m}$.*

Proof. Since the order of φ is N, the set $\{f_a(x) : a \in \mathbb{F}_{r^m}\}$ has at most $N+1$ distinct polynomials. For any $a \in \mathbb{F}_{r^m}$, $f_a(x) = -1$ has at most two solutions in $\mathbb{F}_q$. Theorefore, all these equations in $\{f_a(x) = -1 : a \in \mathbb{F}_{r^m}\}$ have at most $2(N+1)$ solutions over $\mathbb{F}_q$. Since $q > 2(N+1)$, there exists an element $v \in \mathbb{F}_q$ such that v is not a solution of any equation $f_a(x) = -1$, i.e., there exists $v \in \mathbb{F}_q$ satisfying $\lambda_a = f_a(v) \neq -1$ for any $a \in \mathbb{F}_{r^m}$. □

Based on the discussion above, we can easily get the following theorem.

Theorem 4.6. *Let r be a prime number and m be a positive integer. Assume that $N > 1$ is a positive integer and $N|(r^m-1)$. Let q be a power of prime p and $(p,r) = 1$. Assume that $N|(q-1)$. Let $C := C_{(\varphi,v)}$ be the linear code over $\mathbb{F}_q$ with generator matrix $[I_{r^m}, P]$. If $q > 2(N+1)$, then there exists $v \in \mathbb{F}_q$ such that C is an $[2r^m, r^m]$ LCD code over $\mathbb{F}_q$.*

Proof. By Lemmas 2.7 and 4.5, we can easily obtain the desired results. So we omit the detail here. □

Next, we present an example to explain the result of Theorem 4.6.

Example 4.7. *Let $r = 2, m = 2, N = 3, p = 5$ and $q = 25$. Let $\mathbb{F}_{25}^* = \langle\beta\rangle$, where β is a fixed primitive element of $\mathbb{F}_{25}^*$. Taking $v = \beta^2$. It is easy to check that q, r, N satisfy the conditions in Theorem 4.6. Then C is an $[8, 4, 4]$ LCD code over $\mathbb{F}_{25}$ with generator matrix $[I_4, P]$, where*

$$P = \begin{pmatrix} \beta^2 & \beta^{16} & \beta^8 & 1 \\ \beta^{16} & \beta^2 & 1 & \beta^8 \\ \beta^8 & 1 & \beta^2 & \beta^{16} \\ 1 & \beta^8 & \beta^{16} & \beta^2 \end{pmatrix},$$

which is an almost MDS code. Moreover, the dual code of C has parameters $[8, 4, 4]$, which is also an almost MDS code.

5 The constructions of linear codes with one-dimensional hull

In this section, we present the constructions of linear codes with one-dimensional hull by using the two homomorphisms (1) and (2). In order to construct linear codes with one-dimensional hull over $\mathbb{F}_q$, we hope that there exists $v \in \mathbb{F}_q$ satisfying $\lambda_0 = v^2 = -1$ and $\lambda_a \neq -1$ for any $a \in \mathbb{F}_{r^m}$ by Lemma 2.8. Let q be a power of a prime p. In what follows, we shall consider the construction dividing into two cases $p = 2$ and $p \geq 3$.

5.1 The case $p = 2$

Define $\rho(0) = v = 1$. Then $v^2 = 1 = -1$. We then obtain a $r^m \times r^m$ matrix $P = (p_{ij})$ by

$$p_{ij} = \rho(x_j - x_i),$$

which is defined as (4). It follows from (5) that all eigenvalues of PP^T are given by

$$\lambda_a = \begin{cases} -1, & \text{if } a = 0; \\ -1 + (g(\varphi, \chi_a))^2, & \text{if } a \in \mathbb{F}_{r^m}^*. \end{cases} \tag{8}$$

Therefore, we present the following theorem.

Theorem 5.1. *Let r be an odd prime number and m be a positive integer. Assume that $N > 1$ is a positive integer and $N|(r^m - 1)$. Let q be a power of $p = 2$ and $N|(q - 1)$. Let*

$C := C_{(\varphi,1)}$ be the linear code over $\mathbb{F}_q$ with generator matrix $[I_{r^m}, P]$. Then C is a $[2r^m, r^m]$ linear code over $\mathbb{F}_q$ with one-dimensional hull.

Proof. It follows from (8) that all eigenvalues of PP^T are -1 when $a = 0$ and $-1+(g(\varphi,\chi_a))^2$ when $a \in \mathbb{F}_{r^m}^*$. By using Lemma 2.8, we just have to prove that $-1 + (g(\varphi,\chi_a))^2 \neq -1$ for any $a \in \mathbb{F}_{r^m}^*$. Note that the result $g(\varphi,\chi_a)\overline{g(\varphi,\chi_a)} = r^m$ for any $a \in \mathbb{F}_{r^m}^*$ from Lemma 2.4. Then $g(\varphi,\chi_a) \neq 0$ and $\overline{g(\varphi,\chi_a)} \neq 0$ for any $a \in \mathbb{F}_{r^m}^*$. Hence, $(g(\varphi,\chi_a))^2 \neq 0$ and $-1 + (g(\varphi,\chi_a))^2 \neq -1$ for any $a \in \mathbb{F}_{r^m}^*$. The desired conclusion then follows. □

Here, we give a concrete example as follows.

Example 5.2. *Let $r = 13, m = 1, N = 3, p = 2$ and $q = 4$. Let $\mathbb{F}_4^* = \langle\beta\rangle$, where β is a fixed primitive element of $\mathbb{F}_4^*$. It is easy to check that q, r, N satisfy the conditions in Theorem 5.1. Then C is a $[26, 13, 8]$ linear code over $\mathbb{F}_4$ with one-dimensional hull and its generator matrix $[I_{13}, P]$, where*

$$P = \begin{pmatrix}
1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 \\
1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta \\
\beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta \\
\beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 \\
\beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 \\
1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 \\
\beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1 & \beta^2 \\
\beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2 & 1 \\
1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta & \beta^2 \\
\beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta & \beta \\
\beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1 & \beta \\
\beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1 & 1 \\
1 & \beta & \beta & \beta^2 & 1 & \beta^2 & \beta^2 & 1 & \beta^2 & \beta & \beta & 1 & 1
\end{pmatrix}.$$

Moreover, the hull of C is a $[26, 1, 26]$ cyclic code over $\mathbb{F}_4$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

5.2 The case $p \geq 3$

In this subsection, we let $\mathbb{F}_q^* = \langle\beta\rangle$, where β is a fixed primitive element of $\mathbb{F}_q^*$. Assume that $4|(q-1)$.

Define $\rho(0) = v = \beta^{\frac{q-1}{4}}$. Then $v^2 = (\beta^{\frac{q-1}{4}})^2 = \beta^{\frac{q-1}{2}} = -1$. We then obtain a $r^m \times r^m$ matrix $P = (p_{ij})$ by

$$p_{ij} = \rho(x_j - x_i),$$

which is defined as (4). In addition, $\varphi(-1) = \varphi(\alpha^{\frac{r^m-1}{2}}) = u^{\frac{r^m-1}{2}} = (\beta^{\frac{q-1}{N}})^{\frac{r^m-1}{2}} = (\beta^{\frac{q-1}{2}})^{\frac{r^m-1}{N}} = (-1)^{\frac{r^m-1}{N}}$. When $\frac{r^m-1}{N}$ is odd, $\varphi(-1) = -1$; when $\frac{r^m-1}{N}$ is even, $\varphi(-1) = 1$.

Combined with (5), when $\frac{r^m-1}{N}$ is odd, we have

$$\lambda_a = \begin{cases} -1, & \text{if } a = 0; \\ -1 - (g(\varphi, \chi_a))^2, & \text{if } a \in \mathbb{F}_{r^m}^*; \end{cases} \tag{9}$$

when $\frac{r^m-1}{N}$ is even, we get

$$\lambda_a = \begin{cases} -1, & \text{if } a = 0; \\ -1 + (2v + g(\varphi, \chi_a))g(\varphi, \chi_a), & \text{if } a \in \mathbb{F}_{r^m}^*. \end{cases} \tag{10}$$

Collecting all discussions above, we first present the sufficient conditions for constructing linear codes with one-dimensional hull when $\frac{r^m-1}{N}$ is odd.

Theorem 5.3. *Let r be a prime number and m be a positive integer. Assume that $N > 1$ is a positive integer and $N|(r^m - 1)$. Let q be a power of prime p and $(p, r) = 1$. Assume that $N|(q-1)$ and $4|(q-1)$. Let $C := C_{(\varphi, \beta^{\frac{q-1}{4}})}$ be the linear code over $\mathbb{F}_q$ with generator matrix $[I_{r^m}, P]$. When $\frac{r^m-1}{N}$ is odd, C is a $[2r^m, r^m]$ linear code over $\mathbb{F}_q$ with one-dimensional hull.*

Proof. The proof is similar to that of Theorem 5.1 and omitted here. □

Example 5.4. *Let $r = 3, m = 2, N = 8, p = 7$ and $q = 49$. Let $\mathbb{F}_{49}^* = \langle \beta \rangle$, where β is a fixed primitive element of $\mathbb{F}_{49}^*$. It is easy to check that q, r, N satisfy the conditions in Theorem 5.3. Then C is a $[18, 9, 8]$ linear code over $\mathbb{F}_{49}$ with one-dimensional hull and its generator matrix $[I_9, P]$, where*

$$P = \begin{pmatrix} \beta^{12} & \beta^{42} & \beta^{6} & \beta^{30} & 1 & \beta^{36} & \beta^{18} & \beta^{12} & 6 \\ \beta^{18} & \beta^{12} & 1 & \beta^{12} & \beta^{36} & \beta^{6} & \beta^{42} & 6 & \beta^{30} \\ \beta^{30} & 6 & \beta^{12} & \beta^{6} & \beta^{18} & \beta^{42} & \beta^{12} & 1 & \beta^{36} \\ \beta^{6} & \beta^{36} & \beta^{30} & \beta^{12} & \beta^{12} & 6 & 1 & \beta^{18} & \beta^{42} \\ 6 & \beta^{12} & \beta^{42} & \beta^{36} & \beta^{12} & \beta^{18} & \beta^{30} & \beta^{6} & 1 \\ \beta^{12} & \beta^{30} & \beta^{18} & 1 & \beta^{42} & \beta^{12} & 6 & \beta^{36} & \beta^{6} \\ \beta^{42} & \beta^{18} & \beta^{36} & 6 & \beta^{6} & 1 & \beta^{12} & \beta^{30} & \beta^{12} \\ \beta^{36} & 1 & 6 & \beta^{42} & \beta^{30} & \beta^{12} & \beta^{6} & \beta^{12} & \beta^{18} \\ 1 & \beta^{6} & \beta^{12} & \beta^{18} & 6 & \beta^{30} & \beta^{36} & \beta^{42} & \beta^{12} \end{pmatrix}.$$

Moreover, the hull of C is a $[18, 1, 18]$ quasi-cyclic code of index 2 over $\mathbb{F}_{49}$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{12} \end{pmatrix}.$$

Compared with Example 2(2) in [18], the linear code C over $\mathbb{F}_{49}$ with one-dimensional hull we obtained has better parameters than its parameters. In other words, the linear code C of the length 18 with the dimension 9 has the minimal distance 8, while the linear code C of the length 18 with the dimension 9 in [18, Example 2(2)] has the minimal distance 7. That is to say, the linear code C over $\mathbb{F}_{49}$ with one-dimensional hull we obtained is also considered new.

Example 5.5. *Let $r = 7, m = 1, N = 6, p = 5$ and $q = 25$. Let $\mathbb{F}_{25}^* = \langle\beta\rangle$, where β is a fixed primitive element of $\mathbb{F}_{25}^*$. It is easy to check that q, r, N satisfy the conditions in Theorem 5.3. Then C is a $[14, 7, 7]$ linear code over $\mathbb{F}_{25}$ with one-dimensional hull and its generator matrix $[I_7, P]$, where*

$$P = \begin{pmatrix} 2 & 1 & \beta^8 & \beta^4 & \beta^{16} & \beta^{20} & 4 \\ 4 & 2 & 1 & \beta^8 & \beta^4 & \beta^{16} & \beta^{20} \\ \beta^{20} & 4 & 2 & 1 & \beta^8 & \beta^4 & \beta^{16} \\ \beta^{16} & \beta^{20} & 4 & 2 & 1 & \beta^8 & \beta^4 \\ \beta^4 & \beta^{16} & \beta^{20} & 4 & 2 & 1 & \beta^8 \\ \beta^8 & \beta^4 & \beta^{16} & \beta^{20} & 4 & 2 & 1 \\ 1 & \beta^8 & \beta^4 & \beta^{16} & \beta^{20} & 4 & 2 \end{pmatrix},$$

which is an almost MDS code. Moreover, the hull of C is a $[14, 1, 14]$ quasi-cyclic code of index 2 over $\mathbb{F}_{25}$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix}.$$

Next, we turn to the sufficient conditions for constructing linear codes with one-dimensional hull when $\frac{r^m-1}{N}$ is even.

Theorem 5.6. *Let r be a prime number and m be a positive integer. Assume that $N > 1$ is a positive integer and $N|(r^m - 1)$. Let q be a power of prime p and $(p, r) = 1$. Assume that $N|(q - 1)$ and $4|(q - 1)$. Let $C := C_{(\varphi, \beta^{\frac{q-1}{4}})}$ be the linear code over $\mathbb{F}_q$ with generator matrix $[I_{r^m}, P]$. When $\frac{r^m-1}{N}$ is even and $2v + g(\varphi, \chi_a) \neq 0$ for all $a \in \mathbb{F}_{r^m}^*$, C is a $[2r^m, r^m]$ linear code over $\mathbb{F}_q$ with one-dimensional hull.*

Proof. It follows from (10) that all eigenvalues of PP^T are -1 when $a = 0$ and $-1 + (2v + g(\varphi, \chi_a))g(\varphi, \chi_a)$ when $a \in \mathbb{F}_{r^m}^*$. According to Lemma 2.8, we just have to prove that $-1 + (2v + g(\varphi, \chi_a))g(\varphi, \chi_a) \neq -1$ for all $a \in \mathbb{F}_{r^m}^*$.

By utilizing Lemma 2.4 and the proof of Theorem 5.1, we obtain that $g(\varphi, \chi_a) \neq 0$ for any $a \in \mathbb{F}_{r^m}^*$. When $2v + g(\varphi, \chi_a) \neq 0$ for all $a \in \mathbb{F}_{r^m}^*$, we have $-1 + (2v + g(\varphi, \chi_a))g(\varphi, \chi_a) \neq -1$ for all $a \in \mathbb{F}_{r^m}^*$.

Therefore, the matrix PP^T has an eigenvalue -1 with multiplicity 1. It then follows from Lemma 2.8 that C is a $[2r^m, r^m]$ linear code over $\mathbb{F}_q$ with one-dimensional hull. $\square$

In Theorem 5.6, the condition "$2v + g(\varphi, \chi_a) \neq 0$ for all $a \in \mathbb{F}_{r^m}^*$" is not very straightforward. Hence, we will present the following corollary as a concrete result.

Corollary 5.7. *Let r be a prime number and m be a positive integer. Assume that $N > 1$ is a positive integer and $N|(r^m - 1)$. Let q be a power of odd prime p and $(p, r) = 1$. Assume that $N|(q-1)$ and $4|(q-1)$. Let $C := C_{(\varphi, \beta^{\frac{q-1}{4}})}$ be the linear code over $\mathbb{F}_q$ with generator matrix $[I_{r^m}, P]$. Let $\frac{r^m-1}{N}$ be even. If $\varphi(q) \neq 1$, then C is a $[2r^m, r^m]$ linear code over $\mathbb{F}_q$ with one-dimensional hull.*

Proof. Since $\frac{r^m-1}{N}$ is even and it follows from (10) that all eigenvalues of PP^T are -1 when $a = 0$ and $-1 + (2v + g(\varphi, \chi_a))g(\varphi, \chi_a)$ when $a \in \mathbb{F}_{r^m}^*$. Suppose that $2v + g(\varphi, \chi_a) = 0$ for some $a \in \mathbb{F}_{r^m}^*$. Then $g(\varphi, \chi_a) = -2v \in \mathbb{F}_p$ when $p \equiv 1 \pmod 4$ and $g(\varphi, \chi_a) = -2v \in \mathbb{F}_{p^2}$ when $p \equiv 3 \pmod 4$. In addition,

$$\begin{aligned}
(g(\varphi, \chi_a))^q &= \left(\sum_{x \in \mathbb{F}_{r^m}^*} \varphi(x)\chi_a(x) \right)^q \\
&= g(\varphi^q, \chi_{aq}) \\
&= g(\varphi, \chi_{aq}) \\
&= \varphi(q^{-1}) g(\varphi, \chi_a) \\
&= \varphi(q)^{-1} g(\varphi, \chi_a)
\end{aligned}$$

by $N|(q-1)$ and Section 3(3). If $\varphi(q) \neq 1$, then $(g(\varphi, \chi_a))^q \neq g(\varphi, \chi_a)$, i.e., $g(\varphi, \chi_a) \notin \mathbb{F}_q$.

When $p \equiv 1 \pmod 4$, $\mathbb{F}_p \subseteq \mathbb{F}_q$, which implies that $g(\varphi, \chi_a) \notin \mathbb{F}_p$. It is a contradiction.

When $p \equiv 3 \pmod 4$, $\mathbb{F}_{p^2} \subseteq \mathbb{F}_q$ by $4|(q-1)$, which implies that $g(\varphi, \chi_a) \notin \mathbb{F}_{p^2}$. It is a contradiction.

Hence, $2v + g(\varphi, \chi_a) \neq 0$. By using Lemma 2.4, we obtain that $g(\varphi, \chi_a) \neq 0$. Then $-1 + (2v + g(\varphi, \chi_a))g(\varphi, \chi_a) \neq -1$ for all $a \in \mathbb{F}_{r^m}^*$. Thus the matrix PP^T has an eigenvalue -1 with multiplicity 1. It then follows from Lemma 2.8 that the desired result then follows. $\square$

We now employ Corollary 5.7 to present a example as follows.

Example 5.8. *Let $r = 7, m = 1, N = 3, p = 5$ and $q = 25$. Let $\mathbb{F}_{25}^* = \langle \beta \rangle$, where β is a fixed primitive element of $\mathbb{F}_{25}^*$. It is easy to check that q, r, N satisfy the conditions in Corollary 5.7. Then C is a $[14, 7, 6]$ linear code over $\mathbb{F}_{25}$ with one-dimensional hull and its generator*

matrix $[I_7, P]$*, where*

$$P = \begin{pmatrix} 2 & 1 & \beta^{16} & \beta^8 & \beta^8 & \beta^{16} & 1 \\ 1 & 2 & 1 & \beta^{16} & \beta^8 & \beta^8 & \beta^{16} \\ \beta^{16} & 1 & 2 & 1 & \beta^{16} & \beta^8 & \beta^8 \\ \beta^8 & \beta^{16} & 1 & 2 & 1 & \beta^{16} & \beta^8 \\ \beta^8 & \beta^8 & \beta^{16} & 1 & 2 & 1 & \beta^{16} \\ \beta^{16} & \beta^8 & \beta^8 & \beta^{16} & 1 & 2 & 1 \\ 1 & \beta^{16} & \beta^8 & \beta^8 & \beta^{16} & 1 & 2 \end{pmatrix}.$$

Moreover, the hull of C *is a* $[14, 1, 14]$ *quasi-cyclic code of index* 2 *over* $\mathbb{F}_{25}$ *with generator matrix*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix}.$$

Furthermore, some optimal or almost optimal LCD codes (resp. linear codes with one-dimensional hull) derived from Theorems 4.1 and 4.6 (resp. Theorems 5.1, 5.3 and Corollary 5.7) are listed in Table 1 by Magma [2].

Remark 5.9. *In Table 1, optimal linear codes with one-dimensional hull in [18, Section A] can also be obtained by our construction methods when* $N = 2$ *(see the first row, fourth row and fifth row of Table 1), which implies that our results contain partial results in [18, Section A]. When* $N > 2$*, the linear codes are different from those in [18, Section A]. In addition, although the second and third low parameters of Table 1 are the same, we verified by Magma that the two codes are not equivalent.*

6 The minimum distance of the linear code $C_{(\varphi,v)}$

In this section, we discuss the lower bound on the minimum distance of linear code $C := C_{(\varphi,v)}$ with generator matrix $G = [I_{r^m}, P]$ defined in Section 3.

Assume that q is a power of odd prime p and $N = 2$. Let $\mathbb{F}_{r^m} = \{x_i : 1 \le i \le r^m\}$, where $x_1, \cdots, x_{\frac{r^m-1}{2}}$ are non-zero squares in $\mathbb{F}_{r^m}$, $x_{\frac{r^m+1}{2}}, \cdots, x_{r^m-1}$ are non-squares in $\mathbb{F}_{r^m}$ and $x_{r^m} = 0$. From Section 3, we have $P\eta_a = \theta_a \eta_a$ for any $a \in \mathbb{F}_{r^m}$, where $\theta_a := \sum_{y \in \mathbb{F}_{r^m}} \rho(y)\chi_a(y)$ and $\eta_a := (\chi_a(x_1), \chi_a(x_2), \cdots, \chi_a(x_{r^m}))^T$. Let $Q := (\eta_{x_1}, \eta_{x_2}, \cdots, \eta_{x_{r^m}})$. Then

$$\begin{aligned} PQ &= (P\eta_{x_1}, P\eta_{x_2}, \cdots, P\eta_{x_{r^m}}) \\ &= (\theta_{x_1}\eta_{x_1}, \theta_{x_2}\eta_{x_2}, \cdots, \theta_{x_{r^m}}\eta_{x_{r^m}}) \\ &= (\eta_{x_1}, \eta_{x_2}, \cdots, \eta_{x_{r^m}})\Lambda \\ &= Q\Lambda, \end{aligned}$$

where

$$\Lambda = \begin{pmatrix} \theta_{x_1} & & & \\ & \theta_{x_2} & & \\ & & \ddots & \\ & & & \theta_{x_{r^m}} \end{pmatrix} \text{ is a diagonal matrix.}$$

Note that when $v = 0$,

$$\theta_a = \begin{cases} 0, & \text{if } a = 0; \\ \varphi(a^{-1})g(\varphi, \chi_1), & \text{if } a \in \mathbb{F}_{r^m}^*. \end{cases}$$

Let's just say $g := g(\varphi, \chi_1)$ for convenience.

It is easy to know that

$$\Lambda = g(\varphi, \chi_1) \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & -1 & & & & \\ & & & & \ddots & & & \\ & & & & & -1 & & \\ & & & & & & 0 \end{pmatrix}. \tag{11}$$

It follows the definition of the linear code C that C can be expressed in the following form:

$$C \quad = \quad \{c(\boldsymbol{k}) = \boldsymbol{k}G, \boldsymbol{k} \in \mathbb{F}_q^{r^m}\}, \text{where } \boldsymbol{k} = (k_1, k_2, \cdots, k_{r^m}).$$

For any codeword $c(\boldsymbol{k})$ in C, we have

$$\begin{aligned} c(\boldsymbol{k}) &= \boldsymbol{k}G \\ &= \boldsymbol{k}(I_{r^m}, P) \\ &= (\boldsymbol{k}, \boldsymbol{k}P) \\ &= (\boldsymbol{k}, \boldsymbol{l}), \text{where } \boldsymbol{l} := \boldsymbol{l}(\boldsymbol{k}) = \boldsymbol{k}P \\ &= (k_1, k_2, \cdots, k_{r^m}, l_1, l_2, \cdots, l_{r^m}). \end{aligned}$$

Multiply both sides of the equation $\boldsymbol{l} = \boldsymbol{k}P$ by the matrix Q, we obtain

$$\boldsymbol{l}Q = \boldsymbol{k}PQ = \boldsymbol{k}Q\Lambda.$$

Based on the above discussion and combined with Eq. (11), we have the following three equations:

$$\begin{aligned}(l_1 - gk_1, \cdots, l_{r^m} - gk_{r^m})(\eta_{x_1}, \cdots, \eta_{x_{\frac{r^m-1}{2}}}) &= \mathbf{0};\\ (l_1 + gk_1, \cdots, l_{r^m} + gk_{r^m})(\eta_{x_{\frac{r^m+1}{2}}}, \cdots, \eta_{x_{r^m-1}}) &= \mathbf{0};\\ l_1 + \cdots + l_{r^m} &= 0.\end{aligned}$$

In view of the above three equations, we present the following theorem. Before we do that, let's give some definitions. We define $\begin{pmatrix} \mu_{x_1} \\ \vdots \\ \mu_{x_{r^m}} \end{pmatrix} := (\eta_{x_1}, \cdots, \eta_{x_{\frac{r^m-1}{2}}})$ and $\begin{pmatrix} \nu_{x_1} \\ \vdots \\ \nu_{x_{r^m}} \end{pmatrix} := (\eta_{x_{\frac{r^m+1}{2}}}, \cdots, \eta_{x_{r^m-1}})$.

Theorem 6.1. *Let $C := C_{(\varphi,0)}$ be a linear code over $\mathbb{F}_q$ with generator matrix $G = [I_{r^m}, P]$ defined by Section 3. Let A be a positive integer. Assume that any A vectors in $\{\mu_{x_1}, \cdots, \mu_{x_{r^m}}\}$ are linearly independent and any A vectors in $\{\nu_{x_1}, \cdots, \nu_{x_{r^m}}\}$ are also linearly independent. Then $d_{min}(C) \geq A + 1$.*

Proof. Suppose that $c(\boldsymbol{k})$ is any codeword in C which satisfies that $\mathrm{wt}(c(\boldsymbol{k})) < A+1$. Note that $c(\boldsymbol{k}) = (\boldsymbol{k}, \boldsymbol{k}P) = (\boldsymbol{k}, \boldsymbol{l}) = (k_1, \cdots, k_{r^m}, l_1, \cdots, l_{r^m})$. Set $\Omega := \{(l_1, k_1), \cdots, (l_{r^m}, k_{r^m})\}$. Let $x = \#\{(l_i, k_i) \in \Omega \mid (l_i, k_i) = (0, 0) \text{ and } 1 \leq i \leq r^m\}$, $y = \#\{(l_i, k_i) \in \Omega \mid \text{ Only one of } l_i \text{ and } k_i \text{ is 0 and } 1 \leq i \leq r^m\}$ and $z = \#\{(l_i, k_i) \in \Omega \mid l_i \neq 0 \text{ and } k_i \neq 0, \text{ and } 1 \leq i \leq r^m\}$. Then we have

$$\begin{cases} x + y + z = r^m \\ 2x + y > 2r^m - A - 1. \end{cases} \tag{12}$$

From (12), we obtain

$$x \;>\; r^m - A - 1. \tag{13}$$

Let $u_i = l_i - gk_i$ and $w_i = l_i + gk_i$, where $1 \leq i \leq r^m$. Then

$$(u_1, \cdots, u_{r^m}) \begin{pmatrix} \mu_{x_1} \\ \vdots \\ \mu_{x_{r^m}} \end{pmatrix} = u_1\mu_{x_1} + \cdots + u_{r^m}\mu_{x_{r^m}} = \mathbf{0} \tag{14}$$

and

$$(w_1, \cdots, w_{r^m}) \begin{pmatrix} \nu_{x_1} \\ \vdots \\ \nu_{x_{r^m}} \end{pmatrix} = w_1\nu_{x_1} + \cdots + w_{r^m}\nu_{x_{r^m}} = \mathbf{0}. \tag{15}$$

According to (13), it is easy to know that there are at least $r^m - A$ zeros in $u_1, \cdots, u_{r^m}$. Similarly, there are also at least $r^m - A$ zeros in $w_1, \cdots, w_{r^m}$. Without loss of generality, let's assume that $u_{A+1} = \cdots = u_{r^m} = 0$. Combined Eq. (14) and $\mu_{x_1}, \cdots, \mu_{x_A}$ are linearly independent, then we have $u_1 = \cdots = u_A = 0$. Hence, we obtain $u_1 = \cdots = u_{r^m} = 0$. Similarly, we also deduce $w_1 = \cdots = w_{r^m} = 0$. Therefore, we get $l_1 = \cdots = l_{r^m} = 0$ and $k_1 = \cdots = k_{r^m} = 0$. Then $c(\boldsymbol{k})$ is a zero codeword. That is to say, for any nonzero codeword c in C, we have $\mathrm{wt}(c) \geq A + 1$. So $d_{min}(C) \geq A + 1$. This completes the proof. □

Remark 6.2. *According to Theorem 6.1, we expect to find the largest A that satisfies the assumption of Theorem 6.1. It is trivial that $A = 1$ satisfies the assumption of Theorem 6.1. When $\frac{r^m-1}{2} \geq 2$ and $m = 1$, it is easy to prove that $A = 2$ satisfies the assumption of Theorem 6.1. Based on the a lot of examples we have tried by Magma, we guess that $A = \frac{r^m-1}{2}$ satisfies the assumption of Theorem 6.1. If this conjecture is correct, then $d_{min}(C) \geq \frac{r^m+1}{2}$. But we fail to prove it. Thus we would like to put it here as an open problem.*

Conjecture 6.3. *Let $p > 3$, r be two distinct prime numbers and m a positive integer. Assume that $N = 2$. Let $C := C_{(\varphi,v)}$ be a linear code over $\mathbb{F}_q$ with generator matrix $G = [I_{r^m}, P]$, where P is defined by Section 3. Then*

(1) When $v = 0$, we have

$$d_{\min}(C) = \begin{cases} 3, & \text{if } r^m = 3; \\ \frac{r^m+5}{2}, & \text{if } r^m \neq 3. \end{cases}$$

(2) When $v \neq 0$ and $r^m \equiv 1 \pmod 4$, we have

$$d_{\min}(C) = \begin{cases} \frac{r^m+1}{2}, & \text{if } v = \pm 1; \\ \frac{r^m+5}{2}, & \text{if } v \neq \pm 1. \end{cases}$$

Remark 6.4. *Example 4.3 and some examples in Table 1 can illustrate the validity of the above results. In fact, we have tried a lot of examples by Magma, the conjecture is also correct. But we fail to prove it. Thus we would like to put it here as a conjecture.*

7 Conclusion

In this paper, we propose a general method to construct LCD codes and linear codes with one-dimensional hull through the homomorphisms from finite fields into finite fields. Based on the eigenvalues of the matrix PP^T, some sufficient conditions for a linear code to be

an LCD code (resp. a linear code with one-dimensional hull) have been presented in this paper. With these conditions, we obtain some optimal and almost optimal LCD codes (resp. linear codes with one-dimensional hull) by Magma [2], which are exhibited in Table 1. Additionally, we also obtain several almost MDS LCD codes (resp. almost MDS codes with one-dimensional hull) (see Examples 4.7 and 5.5).

Compared with [18], their construction methods are specific and special, while our methods are more general and direct. It is mainly reflected in three aspects:

1. In [18], the matrix P studied by the authors satisfies the symmetry property, while the matrix P we employed in this paper is a general matrix whose eigenvalues are completely determined;

2. In [18], the authors constructed linear codes with one-dimensional hull over finite fields by using the generator matrix over quadratic number fields, while we construct them directly by utilizing the generator matrix over finite fields;

3. Taking $N = 2$, we obtain that [18, Theorem 5] is a special of our results in Theorem 5.3 by comparing the constraints. The results of Theorem 5.6 contain [18, Theorems 3 and 4]. In some sense, some of linear codes with one-dimensional hull we constructed may be new when $N > 2$ by comparing with [18] (see Example 5.4). In addition, we present a lower bound on the minimum distance of linear code C over $\mathbb{F}_q$ with generator matrix $G = [I_{r^m}, P]$ when $N = 2$.

We should emphasize that our results apply to $(p, r) = 1$. It would be interesting to extend the results of the present work to $p = r$. The main open problem is Conjecture 6.3. In addition, although there are many LCD codes and linear codes with one-dimensional hull, it seems to be difficult to determine the minimum distances of the codes presented in this paper when $N > 2$. It will be of interest to find other constructions such that the minimum distances of these codes can be determined.

References

[1] E. F. Assmus, J. D. Key, Affine and projective planes, Discret. Math., vol. 83, nos. 2-3, pp. 161-187, 1990.

[2] W. Bosma, J. J. Cannon, C. Fieker and A. Steel, Hand-book of Magma functions, Edition 2.22 5669 pages (2016). http://magma.maths.usyd.edu.au/magma/.

[3] C. Carlet, S. Guilley, Complementary dual codes for counter-measures to side-channel attacks. In: E.R. Pinto et al. (eds.), Coding Theory and Applications. CIM Series in

Mathematical Sciences, vol. 3, pp. 97-105, Springer (2014). J. Adv. Math. Commun., vol. 10, no. 1, pp. 131-150, 2016.

[4] C. Carlet, C. J. Li, S. Mesnager, Linear codes with small hulls in semi-primitive case, Des. Codes Cryptogr., vol. 87, pp. 3063-3075, 2019.

[5] C. Carlet, S. Mesnager, C. M. Tang, Y. F. Qi, R. Pellikaan, Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. IEEE Trans. Inf. Theory, vol. 64, pp. 3010-3017, 2018.

[6] C. Carlet, S. Mesnager, C. M. Tang, Y. F. Qi, Euclidean and Hermitian LCD MDS codes. Des. Codes Cryptogr., vol. 86, pp. 2605-2618, 2018.

[7] C. Carlet, S. Mesnager, C. M. Tang, Y. F. Qi, New characterization and parametrization of LCD codes. IEEE Trans. Inf. Theory, vol. 65, 39-49, 2019.

[8] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, http://www.codetables. de (2019). Accessed 2 Jan 2019.

[9] L. F. Jin, Construction of MDS codes with complementary duals. IEEE Trans. Inf. Theory, vol. 63, pp. 2843-2847, 2017.

[10] L. F. Jin, C. P. Xing, Algebraic geometry codes with complementary duals exceed the asymptotic Gilbert-Varshamov bound, IEEE Trans. Inform. Theory, vol. 64, pp. 6277-6282, 2018.

[11] S. Jitman, and S. Ling, Quasi-abelian codes, Des. Codes Cryptogr., **74**, (2015), 511–531.

[12] J. S. Leon, Computing automorphism groups of error-correcting codes, IEEE Trans. Inform. Theory, vol. 28, pp. 496-511, 1982.

[13] J. S. Leon, Permutation group algorithms based on partition, I: theory and algorithms, J. Symbolic Comput., vol. 12, pp. 533-583, 1991.

[14] X. S. Liu, H. L. Liu, LCD codes over finite chian rings, Finite Fields Their Appl., vol. 34, pp. 1-19, 2015.

[15] X. S. Liu, Y. Fan, H.L. Liu, Galois LCD codes over finite fields. Finite Fields Their Appl., vol. 49, pp. 227-242, 2018.

[16] S. Mesnager, C. M. Tang, Y. F. Qi, Complementary dual algebraic geometry codes, IEEE Trans. Inf. Theory, vol. 64, no. 4, pp. 2390-2397, Apr. 2018.

[17] R. Lidl, H. Niederreiter, P. M. Cohn, *Finite fields*, Cambridge University Press, 1997.

[18] C. J. Li, P. Zeng, Constrctions of linear codes with one-dimensional hull, IEEE Trans. Inf. Theory, vol. 65, no. 3, pp. 1668-1676, 2019.

[19] J. L. Massey, Linear codes with complementary duals, Discrete Math., vols. 106-107, pp. 337-342, Sep. 1992.

[20] L. Q. Qian, X. W. Cao, S. Mesnager, Linear codes with one-dimensional hull associated with Gaussian sums, Cryptogr. Commun. (2020). https://doi.org/10.1007/s12095-020-00462-y.

[21] L. Q. Qian, X. W. Cao, Linear complementary dual codes constructed by general Gaussian sums over finite fields, submitted.

[22] N. Sendrier, Finding the permutation between equivalent codes: the support splitting algorithm, IEEE Trans. Inform. Theory, vol. 46, pp. 1193-1203, 2000.

[23] M. J. Shi, D. T. Huang, L. Sok, P. Solé, Double circulant LCD codes over $\mathbb{Z}_4$, Finite Fields Their Appl., vol. 58, pp. 133-144, 2019.

[24] L. Sok, M. J. Shi, P. Solé, Constructions of optimal LCD codes over large finite fields, Finite Fields Their Appl., vol. 50, pp. 138-153.

[25] N. Sendrier, G. Skersys, On the computation of the automorphism group of a linear code, in: Proceedings of IEEE ISIT2001, Washington, DC, 2001, p. 13.

Table 1: The list of **optimal or almost optimal** linear codes over small fields

	r, m, N	$\mathbb{F}_q$	$[n, k, d]$	Theorems
LCD codes	$r = 13, m = 1, N = 3$	$\mathbb{F}_7$	$[26, 13, 9]^\star$	Theorem 4.1(1)
	$r = 13, m = 1, N = 4$	$\mathbb{F}_5$	$[26, 13, 9]^\star$	Theorem 4.1(1)
	$r = 17, m = 1, N = 8$	$\mathbb{F}_9$	$[34, 17, 12]^*$	Theorem 4.1(1)
	$r = 17, m = 1, N = 4$	$\mathbb{F}_5$	$[34, 17, 11]^*$	Theorem 4.1(1)
	$r = 5, m = 1, N = 2$	$\mathbb{F}_7$	$[10, 5, 5]^\star$	Theorem 4.1(2)
	$r = 7, m = 1, N = 2$	$\mathbb{F}_5$	$[14, 7, 6]^*$	Theorem 4.1(2)
	$r = 11, m = 1, N = 2$	$\mathbb{F}_7$	$[22, 11, 8]^\star$	Theorem 4.1(2)
	$r = 13, m = 1, N = 2$	$\mathbb{F}_5$	$[26, 13, 9]^\star$	Theorem 4.1(2)
	$r = 17, m = 1, N = 2$	$\mathbb{F}_7$	$[34, 17, 11]^\star$	Theorem 4.1(2)
	$r = 17, m = 1, N = 4$	$\mathbb{F}_9$	$[34, 17, 11]^\star$	Theorem 4.1(2)
	$r = 17, m = 1, N = 2$	$\mathbb{F}_5$	$[34, 17, 11]^*$	Theorem 4.1(2)
	$r = 3, m = 1, N = 2$	$\mathbb{F}_7$	$[6, 3, 3]^\star$	Theorem 4.6
	$r = 3, m = 2, N = 2$	$\mathbb{F}_7$	$[18, 9, 7]^\star$	Theorem 4.6
	$r = 5, m = 1, N = 2$	$\mathbb{F}_7$	$[10, 5, 5]^*$	Theorem 4.6
	$r = 11, m = 1, N = 2$	$\mathbb{F}_7$	$[22, 11, 8]^\star$	Theorem 4.6
Linear codes with one-dimensional hull	$r = 7, m = 1, N = 3$	$\mathbb{F}_4$	$[14, 7, 6]^*$	Theorem 5.1
	$r = 3, m = 1, N = 2$	$\mathbb{F}_5$	$[6, 3, 3]^\star$	Theorem 5.3
	$r = 7, m = 1, N = 2$	$\mathbb{F}_5$	$[14, 7, 6]^*$	Theorem 5.3
	$r = 11, m = 1, N = 2$	$\mathbb{F}_9$	$[22, 11, 8]^\star$	Theorem 5.3
	$r = 17, m = 1, N = 4$	$\mathbb{F}_9$	$[34, 17, 11]^\star$	Corollary 5.7
	$r = 17, m = 1, N = 8$	$\mathbb{F}_9$	$[34, 17, 11]^\star$	Corollary 5.7
	$r = 17, m = 1, N = 2$	$\mathbb{F}_5$	$[34, 17, 11]^*$	Corollary 5.7

The codes with asterisk (*) have the property that linear codes are best known q-ary linear codes in [2], which is optimal. The codes with asterisk ($\star$) have the property that linear codes have better parameters according to the Database [2], which is almost optimal in the sense. For example, the linear code over $\mathbb{F}_9$ of the length $n = 10$ with the dimension $k = 5$ has the minimum distance 5, while the code in the Database [2] has the minimum distance 6.