Linearized Reed-Solomon codes and Linearized Wenger graphs

Haode Yan, Chunlei Liu

Abstract

Let \( m, d \) and \( k \) be positive integers such that \( k \leq \frac{m}{e} \), where \( e = (m, d) \). Let \( p \) be an prime number and \( \pi \) a primitive element of \( \mathbb{F}_{p^m} \). To each \( \bar{a} = (a_0, \ldots, a_{k-1}) \in \mathbb{F}_{p^m}^k \), we associate the linearized polynomial

\[
 f_{\bar{a}}(x) = \sum_{j=0}^{k-1} a_j x^{p^j d}.
\]

And, to each \( f_{\bar{a}}(x) \), we associated the sequence

\[
 c_{\bar{a}} = (f_{\bar{a}}(1), f_{\bar{a}}(\pi), \ldots, f_{\bar{a}}(\pi^{p^m-2})).
\]

Let

\[
 C = \{ c_{\bar{a}} \mid \bar{a} \in \mathbb{F}_{p^m}^k \}
\]

be the cyclic code formed by the sequences \( c_{\bar{a}} \)'s. We call the dual code of \( C \) a linearized Reed-Solomon code. The weight distribution of the code \( C \) is determined in the present paper.

Associated to the \( k \)-tuple \( g = (xy, x^{p^d} y, \ldots, x^{p^{(k-1)d}} y) \) of polynomials in \( \mathbb{F}_{p^m}[x, y] \), there is a Wenger graph \( W_{p^m}(g) \). The spectrum of the graph \( W_{p^m}(g) \) is also determined in the present paper.

Key words: cyclic codes, Wenger graphs, linearized polynomials

MSC: 94B15, 05C50, 11T71.

1  INTRODUCTION

Let \( m, d \) and \( k \) be positive integers such that \( k \leq \frac{m}{e} \), where \( e = (m, d) \). Let \( p \) be an prime number and \( \pi \) a primitive element of \( \mathbb{F}_{p^m} \). To each \( \bar{a} = (a_0, \ldots, a_{k-1}) \in \mathbb{F}_{p^m}^k \), we associate the linearized polynomial

\[
 f_{\bar{a}}(x) = \sum_{j=0}^{k-1} a_j x^{p^j d}.
\]

*Dept. of Math., Shanghai Jiao Tong Univ., Shanghai 200240, hdyan@sjtu.edu.cn.
†Corresponding author, Dept. of Math., SJTU, Shanghai 200240, 714232747@qq.com.
And, to each $f_{\vec{a}}(x)$, we associated the sequence
\[c_{\vec{a}} = (f_{\vec{a}}(1), f_{\vec{a}}(\pi), \cdots, f_{\vec{a}}(\pi^{p^m-2})).\]

Let
\[C = \{c_{\vec{a}} \mid \vec{a} \in \mathbb{F}_p^k\}\]
be the cyclic code formed by the sequences $c_{\vec{a}}$’s. We call the dual code of $C$ a linearized Reed-Solomon code. We are interested in the weight distribution of the code $C$. Other kinds of cyclic codes constructed from linearized polynomials were studied in [4,7,11,12].

Our preliminary task is to determine the weight set of the code $C$. The result is the following.

**Theorem 1.1** If $\vec{a} \neq \vec{0}$, then
\[w(c_{\vec{a}}) \in \{p^m - p^r \mid 0 \leq r \leq k - 1\},\]
where $w(c_{\vec{a}})$ is the Hamming weight of $c_{\vec{a}}$. In particular, $w(c_{\vec{a}}) = 0$ if and only if $\vec{a} = 0$.

Our main task is to determine the frequencies
\[n_r = |\{\vec{a} \in \mathbb{F}_p^k \mid w(c_{\vec{a}}) = p^m - p^r\}|, 0 \leq r \leq k - 1.\] (1)

The result is the following.

**Theorem 1.2** We have, for $0 \leq r \leq k - 1$,
\[n_r = \binom{m}{r} \sum_{i=0}^{k-r-1} (-1)^i p^{\binom{i}{2}(i-1)} \left( \frac{m}{i} - r \right) p^m (p^m(k-r-i) - 1),\]
where $\binom{n}{r}_q$ is the number of $i$-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{F}_q^n$.

Associated to the $k$-tuple $g = (xy, x^{p^d}y, \cdots, x^{p^{(k-1)d}}y)$ of polynomials in $\mathbb{F}_p[m][x, y]$, there is a Wenger graph $W_{p^m}(g)$. The spectrum of that Wenger graph will be determined in the last section.

In the study of Gaussian binomial coefficients, we find the following conjecture.

**Conjecture 1.3** We have
\[\left(\frac{u}{i}\right) \sum_{j=0}^{i} q^j \left(\frac{i}{j}\right) q^2 = \left(\frac{i}{j}\right) q^{\prod_{j=0}^{i-1} (1 + q^{u-j})}.\]

2 PROOF OF THEOREM 1.1

Denote the set of all the roots of $f_{\vec{a}}$ by
\[\text{Null}(f_{\vec{a}}) = \{x \in \mathbb{F}_p^m \mid f_{\vec{a}}(x) = 0\}.\]

It is easy to see that
\[w(c_{\vec{a}}) = p^m - |\text{Null}(f_{\vec{a}})|.\] (2)

It follows from the above equality that Theorem 1.1 is equivalent to the following.
Lemma 2.1 If $\vec{a} \neq \vec{0}$, then

$$|\text{Null}(f_{\vec{a}})| \in \{p^r \mid 0 \leq r \leq k-1\}.$$ 

Proof. Suppose that $\vec{a} \neq 0$. Note that $\{x \in \mathbb{F}_{p^m/d/e} \mid f_{\vec{a}}(x) = 0\}$ is a subspace of $\mathbb{F}_{p^m/d/e}$ over $\mathbb{F}_{p^d}$ of dimension $\leq (k-1)$. As $(m, d) = e$, a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_{p^e}$ is also a basis of $\mathbb{F}_{p^m/d/e}$ over $\mathbb{F}_{p^d}$. It follows that

$$\dim_{\mathbb{F}_{p^d}} \text{Null}(f_{\vec{a}}) \leq (k-1).$$

Hence $|\text{Null}(f_{\vec{a}})| \in \{p^r \mid 0 \leq r \leq k-1\}$. Lemma 2.1 is proved. \qed

It is obvious that 2 also implies the following.

Lemma 2.2 For $0 \leq r \leq k-1$, we have

$$n_r = |\{\vec{a} \in \mathbb{F}_{p^m}^k \mid \text{Null}(f_{\vec{a}}) = p^r\}|.$$ 

3 \textbf{q-BINOMIAL MÖBIUS INVERSION FORMULA}

Let $q$ be a prime power. In this section, we prove the $q$-binomial Möbius inversion formula. We begin with the following definition.

Definition 3.1 ($q$-binomial Möbius function) The $q$-binomial Möbius function is a function on the set of finite-dimensional vector spaces over $\mathbb{F}_q$ defined by the formula

$$\mu_q(U) = (-1)^{\dim U} q^{\binom{\dim U}{2}}.$$ 

Lemma 3.2 We have

$$\sum_{V \subseteq U} \mu_q(V) = \begin{cases} 1, & U = \{0\}, \\ 0, & U \neq \{0\}. \end{cases}$$ 

Proof. The lemma follows from the Gaussian binomial formula

$$\prod_{i=0}^{n-1} (1 + q^i t) = \sum_{i=0}^{n} q^{i(i-1)/2} \binom{n}{i}_q t^i,$$

which can be proved by induction on $n$. \qed

Lemma 3.3 ($q$-binomial Möbius inversion formula) Let $f, g$ be functions defined on the set of $\mathbb{F}_q$-vector spaces. We have

$$g(U) = \sum_{V \subseteq U} f(V)$$

if and only if

$$f(U) = \sum_{V \subseteq U} \mu_q(U/V)g(V).$$
Proof. If 
\[ g(U) = \sum_{V \subseteq U} f(V), \]
then, by Lemma 3.2,
\[ \sum_{V \subseteq U} \mu_q(U/V) g(V) = \sum_{V \subseteq U} \mu_q(U/V) \sum_{W \subseteq V} f(W) \]
\[ = \sum_{W \subseteq U} f(W) \sum_{W \subseteq V \subseteq U} \mu_q(U/V) \]
\[ = \sum_{W \subseteq U} f(W) \sum_{X \subseteq U/W} \mu_q(X) \]
\[ = f(U). \]

The converse can be proved similarly. □

4 q-LINEARIZED VAN DER MONDE MATRIX

In this section, we will determine the rank of a q-linearized Van Der Monde matrix.

Definition 4.1 If \( x_1, x_2, \ldots, x_k \) are \( \mathbb{F}_{p^e} \)-linearly independent elements in \( \mathbb{F}_{p^m} \), then matrix
\[
\begin{pmatrix}
x_1 & x_1^{p^d} & \cdots & x_1^{p^{(k-1)d}} \\
x_2 & x_2^{p^d} & \cdots & x_2^{p^{(k-1)d}} \\
\vdots & \vdots & \ddots & \vdots \\
x_k & x_k^{p^d} & \cdots & x_k^{p^{(k-1)d}}
\end{pmatrix}
\]
is called q-linearized Van Der Monde matrix.

The following lemma is a slight generalization of a lemma of Cao-Lu-Wan-Wang-Wang [1].

Lemma 4.2 A q-linearized Van Der Monde matrix is of full rank.

Proof. Let \( H \) be the \( \mathbb{F}_{p^e} \)-subspace of \( \mathbb{F}_{p^m} \) spanned by the elements \( x_1, x_2, \ldots, x_k \). By Lemma 2.1
\[ \{ \vec{a} \in \mathbb{F}_{p^m}^k \mid \text{Null}(f_{\vec{a}}) \supseteq H \} = \{ 0 \}. \]

Now we consider the following homogeneous linear system of equations:
\[
\begin{align*}
a_0 x_1 + a_1 x_1^{p^d} + \cdots + a_{k-1} x_1^{p^{(k-1)d}} &= 0 \\
a_0 x_2 + a_1 x_2^{p^d} + \cdots + a_{k-1} x_2^{p^{(k-1)d}} &= 0 \\
&\vdots \\
a_0 x_k + a_1 x_k^{p^d} + \cdots + a_{k-1} x_k^{p^{(k-1)d}} &= 0
\end{align*}
\]
Obviously, \( \text{Null}(f_{\vec{a}}) \supseteq H \) if and only if \( \vec{a} \) is a solution of the above system, which implies the rank of the coefficient matrix is \( k \). Lemma 4.2 is proved. □

From the above lemma, one immediately deduces the following.
Corollary 4.3 If \( r \leq k \) and \( x_1, x_2, \ldots, x_r \) are \( \mathbb{F}_{p^e} \)-linearly independent elements in \( \mathbb{F}_{p^m} \), then the following matrix of full rank
\[
\begin{pmatrix}
  x_1 & x_1^{p^d} & \cdots & x_1^{p^{(k-1)d}} \\
  x_2 & x_2^{p^d} & \cdots & x_2^{p^{(k-1)d}} \\
  \vdots & \vdots & \ddots & \vdots \\
  x_r & x_r^{p^d} & \cdots & x_r^{p^{(k-1)d}}
\end{pmatrix}
\]

5 PROOF OF THEOREM 1.2

In this section, we shall prove Theorem 1.2. By the theory of Delsarte [3], Theorem 1.2 follows from Theorem 1.1 directly. However we would like to take an alternative approach. We begin with the following notation. For an \( \mathbb{F}_{p^e} \)-subspace \( V \) of \( \mathbb{F}_{p^m} \), we write
\[
C_V = \{ \vec{a} \in \mathbb{F}_{p^m}^k | \text{Null}(f_{\vec{a}}) \supseteq V^\perp \}.
\]

Lemma 5.1 We have
\[
|C_V| = \begin{cases} 
1, & k \leq \dim V^\perp \leq \frac{m}{e}, \\
\mu_{p^e}(V/W)|C_W|, & \dim V^\perp < k.
\end{cases}
\]

Proof. Let \( \{x_1, x_2, \ldots, x_r\} \) be a basis of \( V^\perp \). Then \( C_V \) is precisely the set of \( \vec{a} \in \mathbb{F}_{p^m}^k \) satisfying the following system
\[
\begin{align*}
  a_0x_1 + a_1x_1^{p^d} + \cdots + a_kx_1^{p^{(k-1)d}} &= 0 \\
  a_0x_2 + a_1x_2^{p^d} + \cdots + a_kx_2^{p^{(k-1)d}} &= 0 \\
  \vdots \\
  a_0x_r + a_1x_r^{p^d} + \cdots + a_kx_r^{p^{(k-1)d}} &= 0.
\end{align*}
\]

Lemma 5.1 now follows from Lemma 4.3.

We now prove Theorem 1.2

Proof. For an \( \mathbb{F}_{p^e} \)-subspace \( V \) of \( \mathbb{F}_{p^m} \), we write
\[
S_V = \{ \vec{a} \in \mathbb{F}_{p^m}^k | \text{Null}(f_{\vec{a}}) = V^\perp \}.
\]

By definition,
\[
|C_V| = \sum_{W \subseteq V} |S_W|.
\]

By Lemmas 4.3, 5.2, and 5.1
\[
|S_V| = \sum_{W \subseteq V} \mu_{p^e}(V/W)|C_W| = \sum_{W \subseteq V} \mu_{p^e}(V/W)(|C_W| - 1) = \sum_{W \subseteq V} \mu_{p^e}(V/W)(p^{m(k-\dim W^\perp)} - 1).
\]
By Lemma 2.2 we have
\[
 n_r = \sum_{\dim V^\perp = r} |S_V|
 = \binom{m}{r} \sum_{i=0}^{k-r-1} (-1)^i p^{\binom{i}{2}} \binom{m}{i}^r (p^{m(k-r-i)} - 1).
\]

Theorem 1.2 is proved.

6 LINEARIZED WENGER GRAPHS

Let \( m, d \) and \( k \) be positive integers such that \( k \leq \frac{me}{e} \), where \( e = (m, d) \). Let \( p \) be a prime number. To each \( k \)-tuple \( g = (g_0, g_1, \cdots, g_{k-1}) \) of polynomials in \( \mathbb{F}_p^m[x, y] \), we associate a graph \( W_{p^m}(g) \), which is called the Wenger graph, as follows. Let \( P \) and \( L \) be two copies of \( \mathbb{F}_p^{k+1} \). The vertex set \( V \) of \( W_{p^m}(g) \) is \( P \cup L \). The edge set \( E \) of \( W_{p^m}(g) \) consists of \((p, l) \in P \times L \) satisfying
\[
l_1 + p_1 = g_0(p_0, l_0), \quad l_2 + p_2 = g_1(p_0, l_0), \cdots, \quad l_k + p_k = g_{k-1}(p_0, l_0),
\]
where \( p = (p_0, p_1, \cdots, p_k) \) and \( l = (l_0, l_1, \cdots, l_k) \).

The above definition of Wenger graph was given by Viglione [8]. It is a generalization of the original Wenger graph. The original Wenger graph was introduced by Wenger [10], and was studied by many authors such as Lazebnik-Ustimenko [5,6], Viglione [8,9], and Cioabă-Lazebnik-Li [2].

The Wenger graph we are interested in is the Wenger graph associated to the \( k \)-tuple \( g = (xy, x^d y, \cdots, x^{d(k-1)} y) \). Following Cao-Lu-Wan-Wang-Wang [1], we call that Wenger graph a linearized Wenger graph. We need the following lemma.

Lemma 6.1 (Cao-Lu-Wan-Wang-Wang [1]) Let \( W_{p^m}(g) \) be the Wenger graph associated to the \( k \)-tuple \((f_0(x)y, f_1(x)y, \cdots, f_{k-1}(x)y)\), where \((f_0, f_1, \cdots, f_{k-1})\) is a \( k \)-tuple of polynomials in \( \mathbb{F}_p^m[x] \) such that the map
\[
\mathbb{F}_p^m \to \mathbb{F}_p^k, \quad u \mapsto (f_0(u), f_1(u), \cdots, f_{k-1}(u))
\]
is injective. Then, counting multiplicities, the eigenvalues of \( W_{p^m}(g) \) are
\[
\{ \pm \sqrt{p^mN_{F_\tilde{a}}} \mid \tilde{a} = (a_{-1}, a_0, \cdots, a_{k-1}) \in \mathbb{F}_p^{k+1} \},
\]
where
\[
F_\tilde{a}(x) = a_{-1} + a_0f_0(x) + a_1f_1(x) + \cdots + a_{k-1}f_{k-1}(x),
\]
and
\[
N_{F_\tilde{a}} = |\{ x \in \mathbb{F}_p^m \mid F_\tilde{a}(x) = 0 \}|.
\]
The following theorem generalizes a result of Cao-Lu-Wan-Wang-Wang [1]. It also solves the open problem put forward by Cao-Lu-Wan-Wang-Wang [1].

**Theorem 6.2** Let $W_{p^m}(g)$ the Wenger graph associated to the $k$-tuple

$$g = (xy, x^{p^d}y, \cdots, x^{p^{(k-1)d}}y).$$

Then the eigenvalues of $W_{p^m}(g)$ are

$$0, \pm p^m, \pm \sqrt{p^{m+cr}}, 0 \leq r \leq k - 1.$$ 

Moreover, the multiplicities of the eigenvalues $\pm p^m$ are 1, the multiplicities of the eigenvalues $\pm \sqrt{p^{m+cr}}$ are $p^{m-cr}n_r$, and the multiplicity of the eigenvalue 0 is

$$\sum_{r=1}^{k-1} (p^m - p^{m-cr})n_r,$$

where the $n_r$'s are the frequencies defined in [7].

**Proof.** It is obvious that

$$N_{F_{\bar{a}}} = \begin{cases} |\text{Null}(f_{\bar{a}})|, & -a_{-1} \in \text{Image}(f_{\bar{a}}), \\ 0, & -a_{-1} \notin \text{Image}(f_{\bar{a}}). \end{cases}$$

By Lemma 2.1, the distinct eigenvalues of $W_{p^m}(g)$ are

$$0, \pm p^m, \pm \sqrt{p^{m+cr}}, 0 \leq r \leq k - 1.$$ 

It remains to calculate the multiplicity of each eigenvalue. First, it is easy to see that the multiplicities of the eigenvalues $\pm p^m$ are 1. Secondly, for each $0 \leq r \leq k - 1$, the multiplicities of the eigenvalues $\pm \sqrt{p^{m+cr}}$ are the number of $\bar{a}$ such that $|\text{Null}(f_{\bar{a}})| = p^{cr}$ and $-a_{-1} \in \text{Image}(f_{\bar{a}})$, which is equal to $p^{m-cr}n_r$ by Lemma 2.2. Finally, the multiplicity of the eigenvalue 0 is equal to

$$\sum_{r=1}^{k-1} (p^m - p^{m-cr})n_r.$$

Theorem 6.2 is proved. ■

**Acknowledgements.** The authors thanks Daqing Wan for mentioning to us the relationship between linearized polynomials and Wenger graphs.

**References**

[1] X. Cao, M. Lu, D. Wan, L. Wang, Q. Wang, Linearized Wenger Graphs, available at http://arxiv.org/abs/1412.0179

[2] S. M. Cioabă, F. Lazebnik, W. Li, On the spectrum of Wenger graphs, J. Combin. Theory, Ser. B, 107 (2014) 132-139.
[3] P. Delsarte, Bilinear forms over a finite field with applications to coding theory, J. Combin. Theory, Ser. A, 25 (1978) 226-241.

[4] K. Feng, J. Luo, Weight distribution of some reducible cyclic codes, Finite Fields Appl. 14 (2) (2008), 390-409.

[5] F. Lazebnik, V. Ustimenko, New examples of graphs without small cycles and of large size, European J. Combin., 14 (1993) 445-460.

[6] F. Lazebnik, V. Ustimenko, Explicit construction of graphs with arbitrary large girth and of large size, Discrete Appl. Math., 60 (1997) 275-284.

[7] H. M. Trachtenberg, On the correlation functions of maximal linear recurring sequences, Ph. D. dissertation, Univ. Southern California, Los Angeles, CA, USA, 1970.

[8] R. Viglione, Properties of some algebraically defined graphs, PhD thesis, University of Delaware, 2002.

[9] R. Viglione, On the diameter of Wenger graphs, Acta Appl. Math. 104 (2008) 173-176.

[10] R. Wenger, Extremal graphs with no $C^4$'s, $C^6$'s, or $C^{10}$'s, J. Combin. Theory Ser. B, 52(1) (1991) 113-116.

[11] D. Zheng, X. Wang, L. Hu, X. Zeng, The weight distribution of a class of $p$-ary cyclic codes, Finite Fields Appl. 16 (5) (2012), 933-945.

[12] Z. Zhou, C. Ding, J. Luo, A. Zhang, A family of five-weight cyclic codes and their weight enumerators, IEEE Trans. Inf. Theory 59 (10) (2013), 6674-6682.