Higher weight distribution of Linearized Reed-Solomon codes

Haode Yan∗, Yan Liu† 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 \( \vec{a} = (a_0, \cdots, a_{k-1}) \in \mathbb{F}_{p^m}^k \), we associate the linearized polynomial

\[
    f_{\vec{a}}(x) = \sum_{j=0}^{k-1} a_j x^{p^{jd}},
\]

as well as the sequence

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

Let

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

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

Key words: cyclic codes, higher weights, linearized polynomials

MSC: 94B15, 05C50, 11T71.

1  INTRODUCTION

Let \( q \) be a prime power, and \( C \) an \([n, k]\)-linear code over \( \mathbb{F}_q \). For an \( \mathbb{F}_q \)-subspace \( H \) of \( C \), the weight of \( H \) is defined to be

\[
    \text{wt}(H) = \# \{ 0 \leq i \leq n-1 \mid c_i \neq 0, \text{ for some } (c_0, c_1, \cdots, c_{n-1}) \in H \}.
\]

If \( \dim H = r \), \( \text{wt}(H) \) is called an \( r \)-dimensional weight of \( C \). If \( r > 1 \), an \( r \)-dimensional weight of \( C \) is called a higher weight of \( C \).

∗Dept. of Math., Shanghai Jiao Tong Univ., Shanghai 200240, hdyan@sjtu.edu.cn.
†Dept. of Math., SJTU, Shanghai 200240, liuyan0916@sjtu.edu.cn.
‡Corresponding author, Dept. of Math., SJTU, Shanghai 200240, 714232747@qq.com.
The notion of higher weights of a linear code was first introduced by Helleseth-Klove-
Mykkeltveit [HKM] in 1977. Motivated by Ozarow-Wyner’s paper [OW] on the cryp-
totographical significance of a linear code in a wire-tap channel, Wei [Wei] rediscovered
the notion of higher weights of a linear code in 1991. Since then, the study of the
higher weights of linear codes has attracted lots of attention, see, for example, the pa-
pers [ABL, BLV, CC, CMN, CH, CLZ, DFGL, DSV, FTW, GO, HKY, 
HKm, HKLY, JL97, JL07, MPP, MR, Mu, SC, SW, SV, TV, GV94a, 
GV94b, GV95a, GV95b, GV95c, GV96, Vl96 and YKS].

For $1 \leq r \leq k$, and for $1 \leq w \leq n$, the number of $r$-dimensional subspaces of $C$ of
weight $i$ is

$$n_{r,w} = \# \{ H \mid \text{wt}(H) = w, \dim H = r \}.$$

Given a $[n, k]$-linear code $C$, it is challenging to determine the set

$$\{ n_{r,w} \mid 1 \leq r \leq k, n-k+r \leq w \leq k \},$$

which is called the higher weight distribution of $C$. The higher weight distribution is
known only for a few classes of codes. Helleseth-Kløve-Mykkeltveit [HKM] determined
the higher weight distribution of the MDS code. Kløve [K] determined the higher weight
distribution of the binary $[23,11]$-Golay code. Helleseth [He] and Hirschfeld-Tsfasman-
Vladut [HTV] determined the higher weight distribution of some other classes of codes.

For $1 \leq r \leq k$, the minimum $r$-dimensional weight of $C$ is

$$d_r = \min \{ \text{wt}(H) \mid \dim H = r \}.$$

Given a $[n, k]$-linear code $C$, it is significant to determine the set $\{ d_1, d_2, \cdots, d_k \}$, which
is called the weight hierarchy of $C$. The weight hierarchy, though an easier problem than
the higher weight distribution, is still known only for a few classes of codes. Helleseth-
Kumar [HK95] determined the weight hierarchy of the Kasami code. Helleseth-Kumar
[HK96], Vlugt [Vl95] and Yang-Li-Feng-Lin [YLFL] determined the weight hierarchy
of irreducible cyclic codes. Heijnen-Pellikaan [HP] determined the weight hierarchy
of the Reed-Muller code. Barbero-Munuera [BM] determined the weight hierarchy of
Hermitian codes. Xiong-Li-Ge determined the weight hierarchy of some reducible cyclic
codes. Wei-Yang [WY], Helleseth-Kløve [HK], Park [Par] and Martinez-Perez-Willems
[MW] determined the weight hierarchy of some product codes.

In the present paper we shall define the linearized Reed-Solomon code and determine
its higher weight distribution. 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 $\vec{a} = (a_0, \cdots, a_{k-1}) \in \mathbb{F}^k_{p^m}$, we associate the linearized polynomial

$$f_{\vec{a}}(x) = \sum_{j=0}^{k-1} a_j x^{p^j d},$$
as well as the sequence
\[ c_{\vec{a}} = (f_{\vec{a}}(1), f_{\vec{a}}(\pi), \ldots, f_{\vec{a}}(\pi^{p^m-2})). \]

From now on we write
\[ C = \{c_{\vec{a}} \mid \vec{a} \in \mathbb{F}_{p^m}^k\}. \]

We call it a linearized Reed-Solomon code. Our preliminary result is the following.

**Theorem 1.1** If \( H \) is a \( \mathbb{F}_{p^m} \)-subspace of \( C \) of dimension \( r > 0 \), then
\[ \text{wt}(H) \in \{p^m - p^i \mid 0 \leq i \leq k - r\}. \]

Our main result is the following.

**Theorem 1.2** If \( r > 0 \), and \( 0 \leq i \leq k - r \), then
\[ n_{r,p^m-p^i} = \binom{m}{i} p^{r-i} \sum_{j=0}^{k-r-i} (-1)^j p^e(j) \binom{k-j-i}{r} p^m \binom{m-i}{j} p^e, \]
where \( \binom{m}{i}_q \) is the number of \( i \)-dimensional \( \mathbb{F}_q \)-subspaces of \( \mathbb{F}_q^m \). In particular, \( d_r = p^m - p^e(k-r) \).

The classical weight distribution of the linearized Reed-Solomon code follows from a result of Delsarte [DEl] on the rank distribution of bilinear forms.

## 2 LINEARIZED VAN DER MONDE MATRIX

In this section, we will introduce the notion of linearized Van Der Monde matrices.

**Lemma 2.1** If \( \vec{a} \in \mathbb{F}_{p^m}^k \) is nonzero, then the number of zeros of \( f_{\vec{a}}(x) \) is \( \leq p^e(k-1) \).

**Proof.** Suppose that \( \vec{a} \neq 0 \). Note that \( \{x \in \mathbb{F}_{p^{md/e}} \mid f_{\vec{a}}(x) = 0\} \) is a subspace of \( \mathbb{F}_{p^{md/e}}^r \) over \( \mathbb{F}_{p^e} \) of dimension \( \leq (k-1) \). As \( (m,d) = e \), a basis of \( \mathbb{F}_{p^m}^r \) over \( \mathbb{F}_{p^e} \) is also a basis of \( \mathbb{F}_{p^{md/e}}^r \) over \( \mathbb{F}_{p^e} \). It follows that, the \( \mathbb{F}_{p^e} \)-space consisting of the zeros of \( f_{\vec{a}}(x) \) is of dimension \( \leq k - 1 \). The lemma now follows. \( \blacksquare \)

**Definition 2.2** If \( (m,d) = e \), and \( x_1, x_2, \ldots, x_k \) 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 \( p^e \)-linearized Van Der Monde matrix.

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

**Lemma 2.3** A linearized Van Der Monde matrix is of full rank.
Proof. Suppose that \((m, d) = e, x_1, x_2, \cdots, x_k\) are \(\mathbb{F}_p^e\)-linearly independent elements in \(\mathbb{F}_{p^m}\), and \(a_0, a_1, \cdots, a_{k-1}\) are elements of \(\mathbb{F}_{p^m}\) such that

\[
a_0 \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} + a_1 \begin{pmatrix} x_1^{d} \\ x_2^{d} \\ \vdots \\ x_k^{d} \end{pmatrix} + \cdots + a_{k-1} \begin{pmatrix} x_1^{p(k-1)d} \\ x_2^{p(k-1)d} \\ \vdots \\ x_k^{p(k-1)d} \end{pmatrix} = 0.
\]

Then \(x_1, x_2, \cdots, x_k\) are zeros of \(f_{\bar{a}}\). It follows that \(|\text{Null}(f_{\bar{a}})| \geq p^k\). By Lemma 2.1 we have \(a_0 = a_1 = \cdots = a_{k-1} = 0\). Therefore

\[
\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix}, \begin{pmatrix} x_1^{d} \\ x_2^{d} \\ \vdots \\ x_k^{d} \end{pmatrix}, \cdots, \begin{pmatrix} x_1^{p(k-1)d} \\ x_2^{p(k-1)d} \\ \vdots \\ x_k^{p(k-1)d} \end{pmatrix}
\]

are linearly independent over \(\mathbb{F}_{p^m}\). It follows that the matrix

\[
\begin{pmatrix} x_1 & x_1^{p} & \cdots & x_1^{p(k-1)d} \\ x_2 & x_2^{p} & \cdots & x_2^{p(k-1)d} \\ \vdots & \vdots & \ddots & \vdots \\ x_k & x_k^{p} & \cdots & x_k^{p(k-1)d} \end{pmatrix}
\]

is of full rank. The lemma is proved. \(\blacksquare\)

The above lemma implies the following.

Corollary 2.4 If \(i \leq k\) and \(x_1, x_2, \cdots, x_i\) are \(\mathbb{F}_p^e\)-linearly independent elements in \(\mathbb{F}_{p^m}\), then the matrix

\[
\begin{pmatrix} x_1 & x_1^{p} & \cdots & x_1^{p(k-1)d} \\ x_2 & x_2^{p} & \cdots & x_2^{p(k-1)d} \\ \vdots & \vdots & \ddots & \vdots \\ x_i & x_i^{p} & \cdots & x_i^{p(k-1)d} \end{pmatrix}
\]

is of full rank over \(\mathbb{F}_{p^m}\).

The above corollary implies the following.

Corollary 2.5 If \(H\) is an \(\mathbb{F}_{p^m}\)-subspace of \(\mathbb{F}_{p^m}^k\) of dimension \(r > 0\), then

\[
Z(H) = \{x \in \mathbb{F}_{p^m} | f_{\bar{a}}(x) = 0, \ \forall \bar{a} \in H\}
\]

an \(\mathbb{F}_p\)-subspace of \(\mathbb{F}_{p^m}\) of dimension \(\leq k - r\).

The above corollary implies the following.

Corollary 2.6 If \(r > 0\), and \(U\) is an \(\mathbb{F}_p\)-subspace of \(\mathbb{F}_{p^m}\) of dimension \(i\), then

\[
|C_{r,U}| = \begin{cases} 
0, & i > k - r, \\
(k-i)_{r}^{p^m}, & i \leq k - r,
\end{cases}
\]
where
\[ C_{r,U} = \{ H \subseteq \mathbb{F}_{p^m}^k \mid Z(H) \supseteq U, \text{ dim}_{p^m} H = r \} . \]

\section{Proof of the Theorems}

It is easy to see that
\[ \text{wt}(H) = p^m - p^e \text{dim}_{p^e} Z(H) . \]

Theorem 1.1 now follows from Corollary 2.5.

We now prove Theorem 1.2. For an \( F_{p^e} \)-subspace \( U \) of \( \mathbb{F}_{p^m} \), we write
\[ S_{r,U} = \{ H \subseteq \mathbb{F}_{p^m}^k \mid Z(H) = U, \text{ dim}_{p^m} H = r \} . \]

Then
\[ n_{r,p^m-p^ei} = \sum_{\text{dim}_{p^e} U = i} |S_{r,U}| . \]

By definition,
\[ |C_{r,W}| = \sum_{W \subseteq U} |S_{r,U}| . \]

By the \( q \)-binomial Möbius inversion formula,
\[ |S_{r,W}| = \sum_{W \subseteq U} (-1)^{\text{dim}U/W} p^{e(\text{dim}U/W)} |C_{r,U}| . \]

It follows that
\[ n_{r,p^m-p^ei} = \binom{m}{r} \frac{k-r-i}{p^e} \sum_{j=0}^{k-r-i} (-1)^j p^{e\binom{j}{r}} \binom{m-i}{j} p^{m-i} . \]

Theorem 1.2 is proved.

\begin{thebibliography}{10}

[ABL] A. Ashikhmin, A. Barg and S. Litsyn, New upper bounds on generalized weights, IEEE Trans. Inform. Theory, 45(4):1258-1263, 1999.

[BM] A. I. Barbero and C. Munuera, The weight hierarchy of Hermitian codes, SIAM J. Discrete Math., 13 (2000), 79-104.

[BLV] M. Bras-Amorós, K. Lee, A. Vico-Oton, New lower bounds on the generalized Hamming weights of AG codes, IEEE Trans. Inform. Theory, 60(10):5930-5937, 2014.

[CLW] X. Cao, M. Lu, D. Wan, L. Wang, Q. Wang, Linearized Wenger Graphs, arXiv:1412.0179

[CC] J. Cheng and C. Chao, On generalized Hamming weights of binary primitive BCH codes with minimum distance one less than a power of two, IEEE Trans. Inform. Theory, 43(1):294-299, 1997.

\end{thebibliography}
[CMN] J. P. Cherdieu, D. J. Mercier and T. Narayaninsamy, On the generalized weights of a class of trace codes, Finite Fields Appl., 7(2):355-371, 2001.

[Ch] H. Chung, The 2-nd generalized Hamming weight of double-error correcting binary BCH codes and their dual codes, In Applied algebra, algebraic algorithms and error-correcting codes, volume 539 of Lecture Notes in Comput. Sci., pages 118-129. Springer, Berlin, 1991.

[CLZ] G. Cohen, S. Litsyn and G. Zémor, Upper bounds on generalized distances, IEEE Trans. Inform. Theory, 40(6):2090-2092, 1994.

[DFGL] M. Delgado, J. I. Farrán, P. A. García-Sánchez and D. Llena, On the weight hierarchy of codes coming from semigroups with two generators, IEEE Trans. Inform. Theory, 60(1):282-295, 2014.

[DEl] P. Delsarte, Bilinear forms over a finite field with applications to coding theory, J. Combin. Theory, Ser. A, 25 (1978) 226-241.

[DSV] I. Duursma, H. Stichtenoth and C. Voß, Generalized Hamming weights for duals of BCH codes, and maximal algebraic function fields, In Arithmetic, geometry and coding theory (Luminy, 1993), pages 53-65. de Gruyter, Berlin, 1996.

[FTW] G. L. Feng, K. K. Tzeng and V. K. Wei, On the generalized Hamming weights of several classes of cyclic codes, IEEE Trans. Inform. Theory, 38(3):1125-1130, 1992.

[GO] C. Güneri and F. Özbudak, Improvements on generalized Hamming weights of some trace codes, Des. Codes Cryptogr., 39(2):215-231, 2006.

[HP] P. Heijnen and R. Pellikaan, Generalized Hamming weights of $q$-ary Reed-Muller codes, IEEE Trans. Inform. Theory, 44 (1998), 181-196.

[He] T. Helleseth, The weight enumerator polynomials of some classes of codes with composite parity-check polynomials, Discrete Math., 20 (1977), 21-31.

[HK] T. Helleseth and T. Kløve, The weight hierarchies of some product codes, IEEE Trans. Inf. Theory 42 (1996), 1029-1034.

[HKLY] T. Helleseth, T.Kløve, V. I. Levenshtein and Ø. Ytrehus, Bounds on the minimum support weights, IEEE Trans. Inform. Theory, 41(2):432-440, 1995.

[HKY] T. Helleseth, T. Kløve and Ø. Ytrehus, Generalized Hamming weights of linear codes, IEEE Trans. Inform. Theory, 38(3):1133-1140, 1992.

[HKM] T. Helleseth, T. Kløve and J. Mykkelset, The weight distribution of irreducible cyclic codes with block length $n_1(q^l - 1)/N$, Discrete Math., 18 (1977), 179-211.

[HK95] T. Helleseth and P. V. Kumar, The weight hierarchy of Kasami codes, Discrete Math., 145 (1995), 133-143.

[HK96] T. Helleseth and P. V. Kumar, On the weight hierarchy of semiprimitive codes, Discrete Math., 152 (1996), 185-190.
[HTV] J. W. P. Hirschfeld, M. A. Tsfasman and S. G. Vladut, The weight hierarchy of higher dimensional hermitian codes, IEEE Trans. Inform. Theory, 40 (1994), 275-278.

[HKm] M. Homma and S. J. Kim, The second generalized Hamming weight for two-point codes on a Hermitian curve, Des. Codes Cryptogr., 50(1):1-40, 2009.

[JL97] H. Janwa and A. K. Lal, On the generalized Hamming weights of cyclic codes, IEEE Trans. Inform. Theory, 43(1):299-308, 1997.

[JL07] H. Janwa and A. K. Lal, On generalized Hamming weights and the covering radius of linear codes, In Applied algebra, algebraic algorithms and error-correcting codes, volume 4851 of Lecture Notes in Comput. Sci., pages 347-356. Springer, Berlin, 2007.

[Kl] T. Kløve, The weight distribution of linear codes over GF(q') having generator matrix over GF(q), Discrete Math., 23 (1978), 159-168.

[MW] C. Martínez-Pérez and W. Willems, The weight hierarchy of product codes, Des. Codes and Crypto. 33 (2004), 95-108.

[MPP] O. Moreno, J. P. Pedersen and D. Polemi, An improved Serre bound for elementary abelian extensions of $F_q(x)$ and the generalized Hamming weights of duals of BCH codes, IEEE Trans. Inform. Theory, 44(3):1291-1293, 1998.

[Mu] C. Munuera, On the generalized Hamming weights of geometric Goppa codes, IEEE Trans. Inform. Theory, 40(6):2092-2099, 1994.

[MR] C. Munuera and D. Ramirez, The second and third generalized Hamming weights of Hermitian codes, IEEE Trans. Inform. Theory, 45(2):709-712, 1999.

[OW] L. H. Ozarow and A. D. Wyner, Wire-tap channel II, AT&T Bell Lab. Tech. J. 63 (1984) 2135-2157.

[Par] J. Y. Park, The weight hierarchy of some product codes, IEEE Trans. Inform. Theory, 46 (2000), 2228-2235.

[Sc] H. G. Schaathun, The weight hierarchy of product codes, IEEE Trans. Inform. Theory, 46(7):2648-2651, 2000.

[SW] H. G. Schaathun and W. Willems, A lower bound on the weight hierarchies of product codes, Discrete Appl. Math., 128(1):251-261, 2003.

[SC] C. Shim, H. Chung, On the second generalized Hamming weight of the dual code of a double-error-correcting binary BCH code, IEEE Trans. Inform. Theory, 41(3):805-808, 1995.

[SV] H. Stichtenoth and C. Voß, Generalized Hamming weights of trace codes, IEEE Trans. Inform. Theory, 40(2):554-558, 1994.

[TV] M. A. Tsfasman and S. G. Vlǎduţ, Geometric approach to higher weights, IEEE Trans. Inform. Theory, 41(6):1564-1588, 1995.

[Gv94a] G. van der Geer and M. van der Vlugt, Generalized Hamming weights of Melas codes and dual Melas codes, SIAM J. Discrete Math., 7(4):554-559, 1994.
[GV94b] G. van der Geer, M. van der Vlugt, On generalized Hamming weights of BCH codes, IEEE Trans. Inform. Theory, 40(2):543-546, 1994.

[GV95a] G. van der Geer and M. van der Vlugt, Fibre products of Artin-Schreier curves and generalized Hamming weights of codes, J. Combin. Theory Ser. A, 70(2):337-348, 1995.

[GV95b] G. van der Geer and M. van der Vlugt, Generalized hamming weights of BCH(3) revisited, IEEE Trans. Inform. Theory, 41(1):300-301, 1995.

[GV95c] G. van der Geer and M. van der Vlugt, The second generalized Hamming weight of the dual codes of double-error correcting binary BCH-codes. Bull. London Math. Soc., 27(1):82-86, 1995.

[GV96] G. van der Geer and M. van der Vlugt, Quadratic forms, generalized Hamming weights of codes and curves with many points, J. Number Theory, 59(1):20-36, 1996.

[Vl95] M. van der Vlugt, The weight hierarchy of irreducible cyclic codes, J. Combin. Theory Ser. A, 71 (1995), 159-167.

[Vl96] M. van der Vlugt, A note on generalized Hamming weights of BCH(2), IEEE Trans. Inform. Theory, 42(1):254-256, 1996.

[Wei] V. K. Wei, Generalized Hamming weights for linear codes, IEEE Trans. Inf. Theory 37 (1991), 1412-1418.

[WY] V. K. Wei and K. Yang, On generalized Hamming weights of product codes, IEEE Trans. Inf. Theory 39 (1993), 1709-1713.

[XLG] M. Xiong, S. Li, and G. Ge, The weight hierarchy of some reducible cyclic codes, \url{arXiv:1504.01274}

[YKS] K. Yang, P. V. Kumar and H. Stichtenoth, On the weight hierarchy of geometric Goppa codes, IEEE Trans. Inf. Theory 59 (2013), 5985-5993.

[YLFL] M. Yang, J. Li, K. Feng and D. Lin, Generalized Hamming weights of irreducible cyclic codes, \url{arXiv:1410.2702}