Annual of Konstantin Preslavsky University of Shumen
vol. XXIV C, 2023, pp. 3 – 7, https://doi.org/10.46687/HTWU8165

SHORTENED AND PUNCTURED CODES AND THEIR HULLS*

STEFKA H. BOUYUKLIEVA

ABSTRACT: *The hull of a linear code is the intersection of the code with its orthogonal complement. We study the relation between the hulls of a linear code, its shortened codes and its punctured codes.*

KEYWORDS: *shortened code, punctured code, hull of a linear code.*

2020 Math. Subject Classification: *94B05*

1 Introduction

Let $\mathbb{F}_q$ be a finite field with q elements and $\mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$. Any k-dimensional subspace of $\mathbb{F}_q^n$ is called a linear q-ary code of length n and dimension k. The vectors in a linear code are called codewords. The (Hamming) *weight* $\mathrm{wt}(x)$ of a vector $x \in \mathbb{F}_q^n$ is the number of its nonzero coordinates. The minimum weight of a linear code C is the minimum nonzero weight of a codeword in C. If C is a linear code of length n, dimension k and minimum weight d, we say that C is an $[n,k,d]$ code. A matrix which rows form a basis of C is called a generator matrix of this code.

Let $(u,v) : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be an inner product in the linear space $\mathbb{F}_q^n$. The dual code of C is $C^\perp = \{u \in \mathbb{F}_q^n : (u,v) = 0 \text{ for all } v \in C\}$. Obviously, $C^\perp$ is a linear $[n,n-k]$ code. The dual distance of C is equal to the minimum weight of its dual code and denoted by $d^\perp$. If $C \subset C^\perp$, the code is called self-orthogonal, and if $C = C^\perp$, the code is self-dual. The intersection $C \cap C^\perp$ is called the hull of the code and denoted by $\mathscr{H}(C)$. The dimension $h(C)$ of the hull can be at least 0 and at most k,

*This paper is (partially) supported by Scientific Research Grant RD-08-32/17.01.2023 of Shumen University

as $h(C) = k$ if and only if the code is self-orthogonal. If $h(C) = 0$, the code is called linear complementary dual (or just LCD) code. So C is an LCD code if $C \cap C^{\perp} = \{0\}$.

This note is organized as follows. In Section 2 we introduce the shortened and punctured codes of a linear code C. In Section 3, we present some theoretical results about the hulls of a linear code and its shortened and punctured codes.

2 Punctured and shortened codes

Let C be a linear $[n,k,d]$ code over the finite field $\mathbb{F}_q$ and T be a set of t coordinate positions. We can puncture C by deleting the coordinates from T in each codeword. The resulting code C^T is still linear but its length is $n-t$. If $t = 1$ and $d > 1$ the the dimension of C^T is k, and its minimum weight is d or $d-1$. If $C(T)$ is the subcode of C consisting of all codewords that have 0's on the set T, puncturing $C(T)$ on T gives the shortened code C_T of C. We need the following result on the punctured and shortened codes of C that is a modification of [2, Theorem 1.5.7].

Theorem 1. *Let C be an $[n,k,d]$ code and T be a set of t coordinates. Then:*

(i) $(C^{\perp})_T = (C^T)^{\perp}$ *and* $(C^{\perp})^T = (C_T)^{\perp}$;

(ii) if $t < d$, then C^T and $(C^{\perp})_T$ have dimensions k and $n-t-k$, respectively.

We focus on the case when $T = \{i\}$, $1 \leq i \leq n$, i.e. puncturing and shortening of a code on one coordinate. Then we denote the punctured code by C^i and the shortened code by C_i. If all codewords in C have 0's in this coordinate, then the punctured and the shortened codes C_i and C^i coincide. In such a case the dual distance of C is 1.

Let $d^{\perp}(C) > 1$ and G be a generator matrix of C, where

$$G = \left(\begin{array}{c|c} 1 & v \\ \hline 0 & \\ \vdots & G_1 \\ 0 & \end{array}\right). \tag{1}$$

Then G_1 is a generator matrix of the shortened code C_1, and the matrix $G^1 = \binom{v}{G_1}$ generates the punctured code C^1.

Let C be a self-orthogonal code over $\mathbb{F}_q$. Obviously, its shortened code on any coordinate set T is also self-orthogonal. However, this is not always true for its punctured codes. It is easy to see that the punctured code C^i is also self-orthogonal if and only if the i-th coordinate in each codeword of C is equal to 0.

3 The hulls

Note that $\mathscr{H}(C) = \mathscr{H}(C^{\perp})$ for any linear code over a finite field.

Theorem 2. *Let C be an $[n,k,1]$ code and $(10\ldots0) \in C$. Then $\mathscr{H}(C) = (0|\mathscr{H}(C_1))$ and $h(C) = h(C_1)$.*

Proof. We have $C = (0|C_1) \cup (1|C_1)$ and $C^{\perp} = (0|C_1^{\perp})$. Now C_1 is a linear $[n-1,k-1,d_1]$ code and $C_1^{\perp}$ has parameters $[n-1,n-k,d^{\perp}]$. If $v \in \mathscr{H}(C)$ then $v = (0,v_1)$, where $v_1 \in C_1 \cap C_1^{\perp} = \mathscr{H}(C_1)$. This proves that $h(C) = h(C_1)$. □

Theorem 3. *If C is a linear q-ary $[n,k,d \geq 2]$ code with dual distance $d^{\perp} \geq 2$ then $h(C_1) = h(C) + \varepsilon$, where $\varepsilon = \pm 1$ or 0.*

Proof. Since $d^{\perp} > 1$, the code C has no zero coordinate. Hence there is a codeword $(1,x) \in C$, and C can be considered as a union of cosets

$$C = \bigcup_{a \in \mathbb{F}_q} (a|ax + C_1).$$

Let $\mathscr{H} = C \cap C^{\perp}$ and $\mathscr{H}_1 = C_1 \cap C_1^{\perp}$. There are two possibilities for $\mathscr{H}$, namely $\mathscr{H} = (0|\mathscr{H}')$ or $\mathscr{H} = \cup_{a \in \mathbb{F}_q}(a|av + \mathscr{H}')$ if $(1,v) \in \mathscr{H}$. In both cases $\mathcal{H}' \subseteq \mathcal{H}_1$. If $\mathcal{H}' = \mathcal{H}_1$ then $\dim\mathcal{H}_1 = \dim\mathcal{H}$ or $\dim\mathcal{H} - 1$.

Let now $\mathcal{H}' \not\equiv \mathcal{H}_1$. Take $y_1, y_2 \in \mathcal{H}_1 \setminus \mathcal{H}'$. Then $(0, y_i) \in C$ and $(a_i, y_i) \in C^\perp$, $a_i \in \mathbb{F}_q^*$, $i = 1,2$. Hence $(0, y_1 - a_1a_2^{-1}y_2) \in \mathcal{H}$ and so $y_1 - a_1a_2^{-1}y_2 \in \mathcal{H}'$. Hence $y_1 \in a_1a_2^{-1}y_2 + \mathcal{H}'$. This shows that $\mathcal{H}_1 = \cup_{a\in\mathbb{F}_q}(a|ay_2 + \mathcal{H}')$ and $\dim\mathcal{H}_1 = \dim\mathcal{H}' + 1$. Since $\dim\mathcal{H}' = \dim\mathcal{H}$ or $\dim\mathcal{H} - 1$, we have $\dim\mathcal{H}_1 = \dim\mathcal{H}$ or $\dim\mathcal{H} + 1$. □

Theorem 3 is proved in [1] only for the binary case.

Corollary 1. *If C is a linear q-ary $[n,k,d \geq 2]$ code with dual distance $d^\perp \geq 2$ then $h(C^1) = h(C) + \varepsilon$, where $\varepsilon = \pm 1$ or 0.*

Proof. According to Theorem 1, we have $C^1 = (C^\perp)_1$. From Theorem 3,

$$\dim\mathcal{H}((C^\perp)_1) = \dim\mathcal{H}(C^\perp) + \varepsilon = \dim\mathcal{H} + \varepsilon = h(C) + \varepsilon.$$

Let us see what happens when the minimum weight of the code C is $d(C) = 2$. Without loss of generality we can take $(110\ldots0) \in C$. We consider two cases for codes with minimum weight 2.

Theorem 4. *Let C be an $[n,k,2]$ q-ary code such that $(110\ldots0) \in C$ and $(1,-1,0\ldots0) \in C^\perp$, and $T = \{1,2\}$. Then*

$$\mathcal{H}(C) = \begin{cases} (00|\mathcal{H}(C_T)) \cup (11|\mathcal{H}(C_T)), & \text{if } \mathrm{char}(\mathbb{F}_q) = 2 \\ (00|\mathcal{H}(C_T)), & \text{if } \mathrm{char}(\mathbb{F}_q) \geq 3 \end{cases}$$

Proof. In this case $C = \bigcup_{a\in\mathbb{F}_q}(aa|C_0)$ and $C^\perp = \bigcup_{a\in\mathbb{F}_q}(a,-a|C_0')$. We consider two cases:

1. Let the characteristic of the field be equal to 2. This means that $q = 2^s$ for an integer $s \geq 1$. Then $-1 = 1$ and $(110\ldots0) \in \mathcal{H}(C)$. If $v_1 \in \mathcal{H}(C_T)$ then $v = (00, v_1) \in \mathcal{H}(C)$ and $(11|v_1) \in \mathcal{H}(C)$. Hence $\mathcal{H}(C) = \bigcup_{a\in\mathbb{F}_q}(aa|\mathcal{H}(C_T))$ and $h(C) = h(C_T) + 1$.

2. Let $\mathrm{char}(\mathbb{F}_q) \geq 3$. If $v_1 \in \mathcal{H}(C_T)$ then $v = (00, v_1) \in C$, but $(b, -b, v_1) \in C^\perp$ for some $b \in \mathbb{F}_q$. But then

$$(b,-b,v_1) - b(1,-1,0\ldots,0) = (0,0,v_1) \in C^\perp$$

and therefore $(00|v_1) \in \mathscr{H}(C)$.

If $(11,v_1) \in \mathscr{H}(C)$ for some $v_1 \in C_T$ then $(11,v_1) \in C^{\perp}$ and so

$$(1,1,v_1)+(1,-1,0\ldots,0) = (2,0,v_1) \in C^{\perp},$$

which is impossible, since the obtained vector is not orthogonal to $(110\ldots0) \in C$. Hence $\mathscr{H}(C) = (00|\mathscr{H}(C_T))$ and $h(C) = h(C_T)$.

Theorem 5. *Let C be an $[n,k,2]$ binary code with $d^{\perp} \geq 3$, $T = \{1,2\}$ and $(110\ldots0) \in C$. Then $h(C) = h(C_T)$.*

Proof. If $v = (aa,v_1) \in \mathscr{H}(C)$ for some $a \in \mathbb{F}_q$ then $(00,v_1) \in C$, so $v_1 \in C_T$. On the other hand, $(aa,v_1) \in C^{\perp}$ and therefore $v_1 \in C_T^{\perp}$. Hence $v_1 \in \mathscr{H}(C_T)$. This shows that $h(C) \leq h(C_T)$. According to Theorem 3, we have $h(C_T) = h(C)$ or $h(C_T) = h(C)+1$. Note that both cases are possible. □

We conclude this note with a corollary for LCD codes with minimum weight 2.

Corollary 2. *Let C be a linear $[n,k,2]$ code over $\mathbb{F}_q$, $q = p^s$ for a prime p, $T = \{1,2\}$ and $(110\ldots0) \in C$. If $p \geq 3$, the code C is LCD if and only if C_T is LCD code. If $p = 2$ and $(110\ldots0) \notin C^{\perp}$, the code C is LCD if and only if C_T is LCD code. If $p = 2$ and $(110\ldots0) \in C^{\perp}$, then C is not an LCD code.*

REFERENCES:

[1] Bouyuklieva S., Optimal binary LCD codes, Des. Codes Cryptogr. 89, (2021), 2445–2461. https://doi.org/10.1007/s10623-021-00929-w

[2] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge Univ. Press, 2003.

Stefka Bouyuklieva
Faculty of Mathematics and Informatics
St. Cyril and St. Methodius University of Veliko Tarnovo
Veliko Tarnovo, Bulgaria
e-mail: stefka@ts.uni-vt.bg