MDS linear codes with one dimensional hull

Lin Sok

Abstract

We define the Euclidean hull of a linear code C as the intersection of C and its Euclidean dual C^{\perp} . The hull with low dimensions gets much interest due to its crucial role in determining the complexity of algorithms for computing the automorphism group of a linear code and checking permutation equivalence of two linear codes. It has been recently proved that any q-ary [n, k] linear code with q > 3 gives rise to a linear code with the same parameters and having zero dimensional Euclidean hull, which is known as a linear complementary dual code. This paper aims to explore explicit constructions of families of MDS linear codes with one dimensional Euclidean hull. We obtain several classes of such codes.

Keywords: Hull, MDS code, generalized Reed-Solomon code, algebraic geometry code, differential algebraic geometry code

I. INTRODUCTION

MDS codes form an optimal family of classical codes. They are closely related to combinatorial designs [23, p. 328], and finite geometries [23, p. 326]. Due to their largest error correcting capability for given length and dimension, MDS codes are of great interest in both theory and practice. The most well-known family of MDS linear codes is that of Reed-Solomon codes. MDS linear codes exist in a very restrict condition on their lengths as the famous MDS conjecture states: for every linear [n, k, n - k + 1] MDS code over \mathbb{F}_q , if 1 < k < q, then $n \le q + 1$, except when q is even and k = 3 or k = q - 1, in which cases $n \le q + 2$. The conjecture was proved by Ball [2] for q a prime. However, for some special classes of linear codes, the conjecture may not be true.

The hull of a linear code was studied by Assmus *et al.* [1] to classify finite projective planes. In coding theory, the hull of a linear code plays a crucial role in determining the complexity of algorithms for computing the automorphism group of a linear code [18] and for checking permutation equivalence of two linear codes [19], [28]. In general, the algorithms have been proved to be very effective if the size of the hull is small. We can summarize the work on the hulls of linear codes as follows. Sendrier [27] determined the expected dimension of the hull of a random [n, k] code when n and k go to infinity. Skersys [30] gave the average dimension of the hulls of cyclic codes. Sangwisut *et al.* [26] gave enumerations of cyclic codes and negacyclic codes of length n with hulls of a given dimension.

There have been a lot of research on constructions of two types of hulls: the one with dimension zero known as linear complementary dual (LCD) code and that with dimension half of the code length known as self-dual code. We refer to [14], [13], [17], [35], [12], [34] for the work on families of MDS self-dual codes and [4], [5], [7], [8], [9], [10], [11], [15], [16], [20], [21], [24], [25], [29], [36] for the LCD codes.

However, there have been very little work on constructing linear codes with other hull dimensions mentioned above except [6], [22]. In this work, we will consider the constructions of MDS linear codes with one dimensional hull. We use tools from algbraic function fields in one variable to study such codes. Sufficient conditions for a code to have one dimensional hull are given, and we explicitly construct many families of MDS linear codes with one dimensional hull. Those families are contained in the following theorem.

Theorem 1. Assume that $q = p^m, m \ge 1$, is a prime power.

- I. If q is even and $n \le q 2$, then there exists a 1-d-hull MDS code with parameters [n, n s 1] for any $1 \le s \le n 3$ (see Corollary 1).
- II. If q > 5 is odd,
 - i. $N \leq q 2$, and set

$$K = \begin{cases} N - 2s - 1 \text{ if } N \text{ is even and } 1 \le s \le \frac{N}{2} - 2, \\ N - 2s - 2 \text{ if } N \text{ is odd and } 0 \le s \le \frac{N+1}{2} - 3 \end{cases}$$

then there exist 1-d-hull MDS codes with parameters [N, K] and [N, N - K] with the following conditions (see Corollary 4):

(1) p|N, (N-1)|(q-1), N even, (2) q square, (N-1)|(q-1), N even, (3) $N|\frac{(q-1)}{2}$, a) N even.

This research work is supported by Anhui Provincial Natural Science Foundation with grant number 1908085MA04. Lin Sok is with School of Mathematical Sciences, Anhui University, 230601 Anhui, P. R. China, (email: soklin_heng@yahoo.com).

b) $q \equiv 1 \pmod{4}$, N odd,

- $\begin{array}{l} \text{(4)} \ 1 \leq r < m, \ \frac{n(p^r+1)}{2(p^r-1)} \ \text{odd}, \ N = (t+1)n, \ n = \frac{q-1}{p^r+1} \ a \ square, \ t \ odd, \ 1 \leq t \leq \lfloor \frac{q-2}{n} \rfloor 1, \\ \text{(5)} \ 1 \leq r < m, \ \frac{n(p^r+1)}{2(p^r-1)} \ even, \ N = (t+1)n, \ n = \frac{q-1}{p^r+1} \ a \ square, \ 1 \leq t \leq \lfloor \frac{q-2}{n} \rfloor 1, \\ \text{(6)} \ 1 \leq r < m, \ N = (t+1)n, \ n = \frac{q-1}{p^r-1} \ a \ square, \ r \mid \frac{m}{2}, \ 1 \leq t \leq p^r 2, \\ \text{(7)} \ m = 2m_0, q_0 = p^{m_0}, \ t \ even, \ 1 \leq t < q_0, \ N = q_0 t, \end{array}$

- (8) $m = 2m_0, q_0 = p^{m_0}, t \text{ odd}, 1 \le t < q_0 \text{ and } 1 \le t \le q_0 1 \text{ for } q = 9, N = q_0 t + 1,$ (9) $m \text{ even}, r = p^{m_0}, m_0 | \frac{m}{2}, N = 2tr^\ell, 0 \le \ell < m/m_0, 1 \le t \le \min((r-1)/2, \lfloor \frac{q-2}{2r^\ell} \rfloor),$

(10)
$$q \equiv 1 \pmod{4}, N = 2p^{\ell}, 0 < \ell < m$$
,

(11) *m* even, $r = p^{m_0}, m_0 | \frac{m}{2}, N = (2t+1)r^{\ell} + 1, 0 \le \ell < m/m_0, 0 \le t \le \min((r-1)/2, | \frac{q-2-r^{\ell}}{2r^{\ell}} |),$

(12)
$$q \equiv 1 \pmod{4}, N = p^{\ell} + 1, 0 < \ell < m,$$

- ii. $n \leq q-1$, p|n and (n-1)|(q-1), then there exist 1-d-hull MDS codes with parameters [n, n-2s+1] and [n, 2s-1]for $1 \le s \le \lfloor \frac{n}{2} \rfloor$ (see Corollary 5),
- iii. $1 \le r < m$ and r|m, then there exist 1-d-hull MDS codes with parameters $[p^r, p^r 2s + 1]$ and $[p^r, 2s 1]$ for $1 \leq s \leq \frac{p^r - 1}{2}$ (see Corollary 6),
- iv. $n \leq (q-2)$, then there exist 1-d-hull MDS codes with parameters as follows (see Corollary 7):
 - i) [n, n-2s+1] and [n, 2s-1] for $1 \le s \le \lfloor (n-1)/2 \rfloor$,
 - ii) [n, n-2s] and [n, 2s] for n even and $1 \le s \le n/2 1$,
- v. $m \ge 2$, $r \le m-1$, r|m, and set $N = (t+1)p^r$ with gcd(p,t+1) = 1 and $1 \le t \le \lfloor \frac{q-1-p^r}{2p^r} \rfloor$, then there exist 1-d-hull MDS codes with parameters [N, N-2s+1] and [N, 2s-1] for $1 \le s \le \lfloor p^r/2 \rfloor$ (see Corollary 8), vi. n|(q-1), and set N = (t+1)n with $1 \le t \le \lfloor \frac{q-n-2}{2n} \rfloor$, then there exist 1-d-hull MDS codes with parameters as
- follows (see Corollary 9):
 - (1) [N, n-2s+1] and [N, tn+2s-1] for $1 \le s \le \lfloor (n-1)/2 \rfloor$, $p \not| (t+1)$,
 - (2) [N, 2n-2s+1] and [N, (t-1)n+2s-1] for $1 \le s \le \lfloor (2n-1)/2 \rfloor$, $p \mid (t+1)$,
 - (3) [N, n-2s] and [N, tn+2s] for n even, $1 \le s \le \lfloor (n-1)/2 \rfloor$, $p \not| (t+1)$,
 - (4) [N, 2n-2s] and [N, (t-1)n+2s] for n even, $1 \le s \le \lfloor (2n-1)/2 \rfloor$, p|(t+1),
 - (5) [N, N-2s+1] and [N, 2s-1] for $1 \le s \le \lfloor (n-1)/2 \rfloor$, $p \not| (t+1)$,
 - (6) [N, N-2s+1] and [N, 2s-1] for $1 \le s \le \lfloor (2n-1)/2 \rfloor$, $p \mid (t+1)$,
 - (7) [N, N-2s] and [N, 2s] for n even, $1 \le s \le \lfloor (n-1)/2 \rfloor$, $p \not| (t+1)$,
 - (8) [N, N-2s] and [N, 2s] for n even, $1 \le s \le \lfloor (2n-1)/2 \rfloor$, $p \lfloor (t+1) \rfloor$.

The paper is organized as follows: Section II gives preliminaries and background on algebraic geometry (AG) codes. Section III provides a characterization of a genus zero AG code to have one dimensional hull. Section IV gives some methods to construct MDS linear codes with one dimensional hull. We give a concluding remark in Section V.

II. PRELIMINARIES

Let \mathbb{F}_q be the finite field with q elements. A linear code of length n and dimension k over \mathbb{F}_q , denoted as q-ary [n, k] code, is a k-dimensional subspace of \mathbb{F}_q^n . The (Hamming) weight wt(x) of a vector $\mathbf{x} = (x_1, \ldots, x_n)$ is the number of nonzero coordinates in it. The minimum distance (or minimum weight) d(C) of C is $d(C) := \min\{\operatorname{wt}(\mathbf{x}) \mid \mathbf{x} \in C, \mathbf{x} \neq \mathbf{0}\}$. The parameters of an [n, k] code with minimum distance d are written [n, k, d]. If C is an [n, k, d] code, then from the Singleton bound, its minimum distance is bounded above by

$$d \le n - k + 1.$$

A code meeting the above bound is called *Maximum Distance Separable* (MDS). The *Euclidean inner product* of $\mathbf{x} =$ (x_1, \ldots, x_n) and $\mathbf{y} = (y_1, \ldots, y_n)$ in \mathbb{F}_q^n is $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^n x_i y_i$. The *dual* of *C*, denoted by C^{\perp} , is the set of vectors orthogonal to every codeword of C under the Euclidean inner product. The (Euclidean) hull of a linear code C is defined as

$$hull(C) = C \cap C^{\perp}.$$

If the hull of a linear code C has dimension s, then we call C an s-d-hull code. With this definition, a linear complementary dual (LCD) code is a 0-d-hull code and a self-dual code of length n is a $\frac{n}{2}$ -d-hull code.

We refer to Stichtenoth [33] for undefined terms related to algebraic function fields. We denote the rational function field of one variable $\mathbb{F}_q(x)$ by \mathcal{F} and the set of places of $\mathbb{F}_q(x)$ by \mathcal{X} . For an element $\alpha \in \mathbb{F}_q$, let P_α denote the zero place of $x - \alpha$ and P_∞ its pole place. A divisor G of \mathcal{F} is a formal sum $\sum_{P \in \mathcal{X}} n_P P$ with only finitely many nonzeros $n_P \in \mathbb{Z}$. The support It is well-known that a nonzero polynomial $f(x) \in \mathbb{F}_q(x)$ can be factorized into irreducible factors as $f(x) = \alpha \prod_{i=1}^{n} p_i(x)^{e_i}$, with $\alpha \in \mathbb{F}_q^*$. Moreover, any irreducible polynomial $p_i(x)$ corresponds to a place, say P_i . We define the valuation of f at P_i as $v_{P_i}(f) := t$ if $p_i(x)^t | f(x)$ but $p_i(x)^{(t+1)} \not| f(x)$.

For $f \in \mathbb{F}_q(x)$, we define

$$\begin{split} (f)_0 &:= \sum_{P \in Z(f)} v_P(f)P, \text{ the zero divisor of } f, \\ (f)_\infty &:= \sum_{P \in N(f)} -v_P(f)P, \text{ the pole divisor of } f, \\ (f) &:= (f)_0 - (f)_\infty, \text{ the principal divisor of } f, \end{split}$$

where Z(f) and N(f) denotes the set of zeros and poles of f, respectively. Hence,

$$(f) = \sum_{P \in \mathcal{X}} v_P(f) P.$$

It is well known that the principal divisor has degree 0.

We say that two divisors G and H are equivalent if G = H + (y) for some rational function $y \in \mathbb{F}_q(x)$. For a divisor G, we define

$$\mathcal{L}(G) := \{ f \in \mathbb{F}_q(x) \setminus \{0\} | (f) + G \ge 0 \} \cup \{0\},\$$

and

$$\Omega(G) := \{ \omega \in \Omega_{\mathcal{F}} \setminus \{0\} | (\omega) - G \ge 0 \} \cup \{0\},\$$

where $\Omega_{\mathcal{F}} := \{ f dx | f \in \mathcal{F} \}$, the set of differential forms.

The dimension of $\mathcal{L}(G)$ is denoted by $\ell(G)$, and is determined by Riemann-Roch's theorem as follows.

Theorem 2. [33, Theorem 1.5.15 (Riemann-Roch)] Let W be a canonical divisor. Then, for each divisor G, the following holds:

$$\ell(G) = \deg G + 1 - g + \ell(W - G),$$

where g is the genus of the smooth algebraic curve.

For a special divisor G, we can determine the dimension of the space $\mathcal{L}(G)$ as follows.

Lemma 1. [33, Corollary 1.4.12] Assume that a divisor G has degree zero. Then G is principal if and only if $\ell(G) = 1$.

For any place $P \neq P_{\infty}$, let $v_P(fdx) := v_P(f)$ and $v_{P_{\infty}}(fdx) := v_{P_{\infty}}(f) - 2$. For an element $\alpha \in \mathbb{F}_q$ and $f \in \mathcal{F}$ with $v_{P_{\alpha}}(f) \geq -1$, it is well known that f(x) can be expanded in the neighborhood of α as follows

$$f(x) = \dots + \frac{a_{-1}}{x - \alpha} + a_0 + a_1(x - \alpha) + \dots$$

If f(x) is in the above form, the residue $Res_{P_{\alpha}}(fdx)$ of fdx at P_{α} is defined to be $Res_{P_{\alpha}}(fdx) := a_{-1}$.

Over $\mathbb{F}_q(x)$, there are q + 1 places of degree one, that is, the zero places P_1, \ldots, P_q and the pole place P_∞ (see [33, Proposition 1.2.1]).

Through out the paper, we let $D = P_1 + \cdots + P_n$, called the rational divisor, where $P_i := P_{\alpha_i}, \alpha_i \in \mathbb{F}_q$, for $1 \le i \le n$, are places of degree one.

For G a divisor with $supp(D) \cap supp(G) = \emptyset$, define the algebraic geometry code by

$$C_{\mathcal{L}}(D,G) := \{ (f(P_1), \dots, f(P_n)) | f \in \mathcal{L}(G) \}$$

and the differential algebraic geometry code as

$$C_{\Omega}(D,G) := \{ (Res_{P_1}(\omega), \dots, Res_{P_n}(\omega)) | \omega \in \Omega(G-D) \}.$$

The parameters of an algebraic geometry code $C_{\mathcal{L}}(D,G)$ is given as follows.

Theorem 3. [33, Corollary 2.2.3] Assume that 2g - 2 < deg(G) < n. Then the code $C_{\mathcal{L}}(D,G)$ has parameters [n,k,d] satisfying

$$k = \deg(G) - g + 1 \text{ and } d \ge n - \deg(G).$$

$$\tag{1}$$

For g = 0, from (1), we get $k = \deg(G) + 1$ and $d \ge n - \deg(G)$ and thus the Singleton bound holds with equality and the code $C_{\mathcal{L}}(D, G)$ is MDS.

For $\mathbf{a} = (\alpha_1, \dots, \alpha_n)$, $\mathbf{v} = (v_1, \dots, v_n) \in \mathbb{F}_q^n$ such that $\alpha_1, \dots, \alpha_n$ are all distinct, and v_1, \dots, v_n are all nonzero, it is well known that the generalized Reed-Solomon code defined by

$$GRS_k(\mathbf{a}, \mathbf{v}) := \{ (v_1 f(\alpha_1), \dots, v_n f(\alpha_n)) | f(x) \in \mathbb{F}_q(x), \deg f \le k - 1 \}$$

is an MDS code. Furthermore, it is shown in [33, Proposition 2.3.3], that any algebraic geometry code $C_{\mathcal{L}}(D,G)$ with $\deg(G) = k - 1$ is equal to the generalized Reed-Solomon code $GRS_k(\mathbf{a}, \mathbf{v})$ defined above.

Moreover, their parameters are related as follows. For all $1 \le i \le n$,

 $\begin{cases} \alpha_i = x(P_i), \\ v_i = u(P_i) \text{ for some } u(x) \in \mathbb{F}_q(x) \text{ satisfying} \\ (u) = (k-1)P_{\infty} - G. \end{cases}$

For $0 \le j \le k - 1$, the vectors

$$(ux^{j}(P_{1}),\ldots,ux^{j}(P_{n}))=(v_{1}\alpha_{1}^{j},\ldots,v_{n}\alpha_{n}^{j})$$

constitute a basis of $C_{\mathcal{L}}(D,G)$, and thus, a generator matrix of $C_{\mathcal{L}}(D,G)$ can be expressed as

(v_1	v_2		v_n		
	$v_1 \alpha_1$	$v_2 \alpha_2$	•••	$v_n \alpha_n$		
	÷	÷		÷		
	$v_1 \alpha_1^{k-2}$	$v_2 \alpha_2^{k-2}$		$v_n \alpha_n^{k-2}$		
ĺ	$v_1 \alpha_1^{k-1}$	$v_2 \alpha_2^{k-1}$	•••	$v_n \alpha_n^{k-1}$	Ϊ	

Equivalence of two algebraic geometry codes is characterized through the associated divisors as follows.

Lemma 2. [33, Proposition 2.2.14] Assume that two divisors G and H are equivalent. Then $\mathcal{L}(G)$ and $\mathcal{L}(H)$ are isomorphic as vector spaces. Moreover, the codes $C_{\mathcal{L}}(D,G)$ and $C_{\mathcal{L}}(D,H)$ are equivalent.

The dual of the algebraic geometry code $C_{\mathcal{L}}(D,G)$ can be described as follows.

Lemma 3. [33, Theorem 2.2.8] With the above notation, the two codes $C_{\mathcal{L}}(D,G)$ and $C_{\Omega}(D,G)$ are dual to each other.

Moreover, the differential code $C_{\Omega}(D,G)$ is determined as follows.

Lemma 4. [33, Proposition 2.2.10] With the above notation, $C_{\Omega}(D,G) = C_{\mathcal{L}}(D,D-G+(\omega))$ for some differential function ω satisfying $v_{P_i}(\omega) = -1$ and $\operatorname{Res}_{P_i}(\omega) = 1$ for $1 \leq i \leq n$.

For simplicity, we let, in the sequel, $h(x) = \prod_{i=1}^{n} (x - \alpha_i)$ and $h'(x) = \frac{dh}{dx}$, the derivative of h with respect to x. Then

$$h'(x) = \sum_{i=1}^{n} \prod_{j=1, j \neq i}^{n} (x - \alpha_j).$$

A simple calculation gives

$$\omega_{h'} := \frac{h'}{h} dx = \left(\frac{1}{x - \alpha_1} + \dots + \frac{1}{x - \alpha_n}\right) dx,$$

and hence, the divisor $(\omega_{h'})$ of $\omega_{h'}$

$$(\omega_{h'}) = (h') - D + (n-2)P_{\infty}$$

satisfies

$$v_{P_i}(\omega_{h'}) = -1, \operatorname{Res}_{P_i}(\omega_{h'}) = 1, \forall 1 \le i \le n.$$

III. CHARACTERIZATION OF ONE DIMENSIONAL HULL

The following lemma gives sufficient conditions for two algebraic geometry codes to have one dimensional intersection subcode.

Lemma 5. With the same notation as above, assume that

(i) A, B, G are divisors such that $A \ge 0, B \ge 0$ and supp(A), supp(B), supp(D) and supp(G) are pairwise disjoint, (ii) deg G < n,

(iii) G - A - B is a principal divisor.

Then $C_{\mathcal{L}}(D, G - A + (z)) \cap C_{\mathcal{L}}(D, G - B + (z))$ is a one-dimensional code for any $z \in \mathbb{F}_q(x)$ satisfying $v_{P_i}(z) = 0$ for all $1 \le i \le n$.

The following lemma gives sufficient conditions for an algebraic geometry code to have one dimensional hull.

Lemma 6. With the same notation as above, assume that

- (i) A, B, G are divisors such that $A \ge 0, B \ge 0$ and supp(A), supp(B), supp(D) and supp(G) are pairwise disjoint, (ii) $\deg G < n$,
- (iii) G A B is a principal divisor,
- (iv) the following condition

$$2G - A - B - (h') - (n-2)P_{\infty} = (y)$$
⁽²⁾

holds for some rational function y such that $y(P_i), \forall 1 \leq i \leq n$, are squares in \mathbb{F}_q^* . Then $C_{\mathcal{L}}(D, G - A + (z))$ is a 1-d-hull code for any $z \in \mathbb{F}_q(x)$ satisfying $(z^2y)(P_i) = 1$ for all $1 \leq i \leq n$.

Proof. Under Condition (i) and the assumption $(z^2y)(P_i) = 1$, the code $C_{\mathcal{L}}(D, G - A + (z))$ is well defined. From the fact that $C_{\mathcal{L}}^{\perp}(D, G - A + (z)) = C_{\Omega}(D, G - A + (z)) = C_{\mathcal{L}}(D, D - G + A - (z) + (\omega_{h'})) = C_{\mathcal{L}}(D, D - G + A - (z) + (h') - D + (n-2)P_{\infty}) = C_{\mathcal{L}}(D, -G + A - (z) + (h') + (n-2)P_{\infty})$. The condition iii) implies that $G - B - (y) - (z) = -G + A + (h') + (n-2)P_{\infty}$. Thus $C_{\mathcal{L}}^{\perp}(D, G - A + (z)) = C_{\mathcal{L}}(D, G - B - (y) - (z)) = C_{\mathcal{L}}(G - B + (z) - (z^2y))$

From Lemma 2, $\mathcal{L}(G - B + (z))$ and $\mathcal{L}(G - B + (z) - (z^2y))$ are isomorphic vector spaces. Define

$$\phi: C_{\mathcal{L}}(D, G - B + (z) - (z^2 y)) \to C_{\mathcal{L}}(D, G - B + (z))$$

such that $\phi(f(P_1), \ldots, f(P_n)) = (\frac{f}{z^2 y}(P_1), \ldots, \frac{f}{z^2 y}(P_n))$. Under the condition $(z^2 y)(P_i) = 1$ for $1 \le i \le n$, we get $\phi(f(P_1), \ldots, f(P_n)) = (f(P_1), \ldots, f(P_n))$, and thus $C_{\mathcal{L}}(D, G-B+(z)-(z^2 y)) = C_{\mathcal{L}}(D, G-B+(z)) = C_{\mathcal{L}}^{\perp}(D, G-A+(z))$. The rest follows from Lemma 5.

IV. CONSTRUCTION OF ONE DIMENSIONAL HULL

By fixing the divisor G, we get the following result.

Theorem 4. Set $G = (n-2)P_{\infty}$. Let a, b be in $\mathbb{F}_q[x]$ such that gcd(a, b) = 1. With the same notation as above, assume that (i) $supp((a)_0) \cap supp(D) = supp((b)_0) \cap supp(D) = \emptyset$,

(*ii*) $\deg a + \deg b = n - 2$,

(iii) $(abh')(P_i), 1 \leq i \leq n$, are nonzero squares in \mathbb{F}_q .

Then $C_{\mathcal{L}}(D, (n-2)P_{\infty} - (a)_0 + (z))$ is a 1-d-hull code for any $z \in \mathbb{F}_q(x)$ satisfying $z(P_i)^2 = (abh')(P_i)$ for all $1 \le i \le n$. Proof. Under the above assumption, we have $2G - A - B - (h') - (n-2)P_{\infty} = G - A - B - (h') = G - (a)_0 - (b)_0 - (h') = \frac{1}{(abh')}$, where $A = (a)_0, B = (b)_0$, and $G - A - B = \frac{1}{(ab)}$ is obviously a principal divisor.

Remark 1. If C is an [n,1] code, then C is a 1-d-hull code if and only if C is self-orthogonal $(C \subset C^{\perp})$.

From now on, we only consider 1-d-hull code with parameters [n, k], where k > 1.

Corollary 1. Assume that q > 4 is even, $n \le q - 2$. Then there exists a 1-d-hull MDS code with parameters [n, n - s - 1] for any $1 \le s \le n - 3$.

Proof. Let $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha \neq \beta$ and the corresponding places $P_{\alpha}, P_{\beta} \notin supp(D)$. Set $a(x) = (x - \alpha)^s, b(x) = (x - \beta)^{n-2-s}$. Since any element in \mathbb{F}_q is a square, we get that $((abh')(\alpha_i))_{1 \leq i \leq n}$ are nonzero square elements in \mathbb{F}_q . \Box

Example 1. For $q = 2^3$, n = 4, 5, 6, and s = 1, using Magma [3], we give three 1-d-hull MDS codes C_1, C_2, C_3 with parameters [4, 2, 3], [5, 3, 3] and [6, 4, 3], respectively as follows.

$$C_{1} = \begin{pmatrix} 1 & 0 & w^{3} & w^{3} \\ 0 & 1 & w^{4} & w^{3} \end{pmatrix}, C_{2} = \begin{pmatrix} 1 & 0 & 0 & w^{4} & w^{6} \\ 0 & 1 & 0 & w & w^{5} \\ 0 & 0 & 1 & w^{3} & w^{6} \end{pmatrix}, C_{3} = \begin{pmatrix} 1 & 0 & 0 & 0 & w^{3} & w^{2} \\ 0 & 1 & 0 & 0 & 1 & w \\ 0 & 0 & 1 & 0 & w^{6} & w^{2} \\ 0 & 0 & 0 & 1 & 1 & w^{2} \end{pmatrix}.$$

Corollary 2. Assume that q > 5 is odd, $n \le q - 2$ and $(h'(P_i))_{1 \le i \le n}$ are nonzero square elements in \mathbb{F}_q .

1) If n is even, then there exists a 1-d-hull MDS code with parameters [n, n-2s-1] for any $1 \le s \le \frac{n}{2} - 2$.

2) If n is odd, $\frac{n-1}{2} \leq q-1$ and $supp((x)_0) \cap supp(D) = \emptyset$, then there exists a 1-d-hull MDS code with parameters [n, n-2s-2] for any $0 \leq s \leq \frac{n+1}{2} - 3$.

Proof. Let $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha \neq \beta$ and the corresponding places $P_{\alpha}, P_{\beta} \notin supp(D)$.

- 1) Set $a(x) = (x \alpha)^{2s}$, $b(x) = (x \beta)^{n-2-2s}$. It is easy to check that $((abh')(\alpha_i))_{1 \le i \le n}$ are nonzero square elements in \mathbb{F}_q .
- 2) Set $a(x) = x(x-\alpha)^{2s}$, $b(x) = (x-\beta)^{n-3-2s}$. For $1 \le i \le n$, take α_i from the set of square elements in \mathbb{F}_q .

Since the dual of an MDS code is again an MDS code, we derive the following

Corollary 3. Assume that q > 5 is odd, $n \le q - 2$ and $(h'(P_i))_{1 \le i \le n}$ are nonzero square elements in \mathbb{F}_q .

- 1) If n is even, then there exists a 1-d-hull MDS code with parameters [n, 2s + 1] for any $1 \le s \le \frac{n}{2} 2$.
- 2) If n is odd, $\frac{n-1}{2} \le q-1$ and $supp((x)_0) \cap supp(D) = \emptyset$, then there exists a 1-d-hull MDS code with parameters [n, 2s+2] for any $0 \le s \le \frac{n+1}{2} 3$.

Corollary 4. Let $q = p^m > 5$ be odd and $N \leq q - 2$. Set

$$K = \begin{cases} N - 2s - 1 \text{ if } N \text{ is even and } 1 \le s \le \frac{N}{2} - 2, \\ N - 2s - 2 \text{ if } N \text{ is odd and } 0 \le s \le \frac{N+1}{2} - 3 \end{cases}$$

Then there exist 1-d-hull MDS codes with parameters [N, K] and [N, N - K] with the following conditions: (1) p|N, (N-1)|(q-1), N even,

(2) q square, (N-1)|(q-1), N even, (3) $N|\frac{(q-1)}{2}$, a) N even, b) $q \equiv 1 \pmod{4}$, N odd, $\begin{array}{l} \text{(4)} \ 1 \leq r < m, \ \frac{n(p^r+1)}{2(p^r-1)} \ \text{odd}, \\ \text{(5)} \ 1 \leq r < m, \ \frac{n(p^r+1)}{2(p^r-1)} \ \text{odd}, \\ N = (t+1)n, \ n = \frac{q-1}{p^r+1} \ a \ \text{square, } t \ \text{odd}, \ 1 \leq t \leq \lfloor \frac{q-2}{n} \rfloor - 1, \\ \text{(5)} \ 1 \leq r < m, \ \frac{n(p^r+1)}{2(p^r-1)} \ \text{even, } \\ N = (t+1)n, \ n = \frac{q-1}{p^r+1} \ a \ \text{square, } 1 \leq t \leq \lfloor \frac{q-2}{n} \rfloor - 1, \\ \text{(6)} \ 1 \leq r < m, \ N = (t+1)n, \ n = \frac{q-1}{p^r-1} \ a \ \text{square, } r \mid \frac{m}{2}, \ 1 \leq t \leq p^r - 2, \\ \text{(7)} \ m = 2m_0, q_0 = p^{m_0}, \ t \ \text{even, } 1 \leq t < q_0, \ N = q_0 t, \\ \text{(8)} \ m = 2m_0, q_0 = p^{m_0}, \ t \ \text{odd}, \ 1 \leq t < q_0 \ \text{odd}, \\ \end{array}$ (8) $m = 2m_0, q_0 = p^{m_0}, t \text{ odd}, 1 \le t < q_0 \text{ and } 1 \le t \le q_0 - 1 \text{ for } q = 9, N = q_0t + 1,$ (9) *m* even, $r = p^{m_0}, m_0 | \frac{m}{2}, N = 2tr^{\ell}, 0 \le \ell < m/m_0, 1 \le t \le \min((r-1)/2, \lfloor \frac{q-2}{2r^{\ell}} \rfloor),$ (10) $1 \pmod{4} N - 2n^{\ell} 0 < \ell$

(10)
$$q \equiv 1 \pmod{4}, N = 2p^{\epsilon}, 0 < \ell < m,$$

(11) *m* even, $r = p^{m_0}, m_0 | \frac{m}{2}, N = (2t+1)r^{\ell} + 1, 0 \le \ell < m/m_0, 0 \le t \le \min((r-1)/2, |\frac{q-2-r^{\ell}}{2r^{\ell}}|),$

(12) $q \equiv 1 \pmod{4}, N = p^{\ell} + 1, 0 < \ell < m.$

Proof. Put

$$h(x) = \prod_{\alpha \in U} (x - \alpha).$$

For each case, it is enough to prove that, for any $\alpha \in U$, $h'(\alpha)$ is a nonzero square in \mathbb{F}_q . Take U as follows.

- for 1), $U = \{ \alpha \in \mathbb{F}_q | \alpha^N = \alpha \},$ for 2), $U = U_N = \{ \alpha \in \mathbb{F}_q | \alpha^N = \alpha \},$
- for 3), $U = U_N = \{ \alpha \in \mathbb{F}_q | \alpha^N = 1 \},\$
- for 4)-6), take $U = U_n \cup \alpha_1 U_n \cup \cdots \cup \alpha_t U_n$, $U_n = \{\alpha \in \mathbb{F}_q | \alpha^n = 1\}$ and $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_q \setminus U_n$.
- for 7)–8), label the elements of \mathbb{F}_{q_0} as a_1, \ldots, a_{q_0} . For some fixed element $\beta \in \mathbb{F}_q \setminus \mathbb{F}_{q_0}$, take $U = \{a_k\beta + a_j | 1 \le k, j \le j \le k\}$ q_0 ,
- for 9)-12), label the element of \mathbb{F}_r as a_0, \ldots, a_{r-1} , take H as an \mathbb{F}_r -subspace and set $H_i = H + a_i\beta$ for some fixed element $\beta \in \mathbb{F}_q \setminus \mathbb{F}_r$. Put $U = H_0 \cup \cdots \cup H_{2t-1}$ or $U = H_0 \cup \cdots \cup H_{2t}$.

For 1)–3), it can be easily checked that $h'(\alpha)$ is a square for any $\alpha \in U$. See also [31, Theorem 2 and Theorem 4].

For 4)–6), it was already checked, in [32, Theorem 3 and Theorem 4], that $h'(\alpha)$ is a square for any $\alpha \in U$. Moreover, in [32], $t \le p^r$ for 4)-5) and $t \le p^r - 2$ for 6). Since $N = (t+1)n \le q-2$, we take $t = \min(\lfloor \frac{q-2}{n} \rfloor - 1, p^r) = \lfloor \frac{q-2}{n} \rfloor - 1$ for 4)-5) and $t = \min(\lfloor \frac{q-2}{n} \rfloor - 1, p^r - 2) = p^r - 2$ for 6).

For 7)–8), it was proved in [35, Theorem 2] that $h'(\alpha)$ is a square for any $\alpha \in U$.

Example 2. From Corollary 4 (3) a), for $q = 3^4$, n = 8, s = 1, we give a 1-d-hull MDS code C_5 with parameters [8, 5, 4] as follows.

$$C_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & w^{49} & w^{57} & w^{35} \\ 0 & 1 & 0 & 0 & 0 & w^{79} & w^{77} & w^{75} \\ 0 & 0 & 1 & 0 & 0 & w^{24} & w^{52} & 2 \\ 0 & 0 & 0 & 1 & 0 & w^{28} & w^{46} & w^{64} \\ 0 & 0 & 0 & 0 & 1 & w^{34} & w^{72} & 1 \end{pmatrix}.$$

Example 3. From Corollary 4 (3) b), for q = 19, n = 9, s = 1, we give a 1-d-hull MDS code C_4 with parameters [9, 5, 5] as follows.

$$C_4 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 2 & 13 & 10 & 5 \\ 0 & 1 & 0 & 0 & 0 & 15 & 8 & 1 & 4 \\ 0 & 0 & 1 & 0 & 0 & 1 & 7 & 6 & 8 \\ 0 & 0 & 0 & 1 & 0 & 16 & 2 & 7 & 8 \\ 0 & 0 & 0 & 0 & 1 & 5 & 12 & 12 & 5 \end{pmatrix}.$$

However when $(h'(P_i)_{1 \le i \le n}$ are not all nonzero square elements in \mathbb{F}_q , we have the following.

Theorem 5. Let q > 5 be an odd prime power. With the same notation as above, assume that $(h')_0 = 2(f)_0 + (g_1)_0 + (g_2)_0$ for some $f, g_1, g_2 \in \mathbb{F}_q[x]$ such that $supp((g_1)_0) \cap supp((g_2)_0) = \emptyset$. Assume further that $n + \deg(g_1) + \deg(g_2) \le q - 1$. Then for any $1 \le s \le \lfloor \frac{(n - \deg(g_1) - \deg(g_2)}{2} \rfloor$, there exists a 1-d-hull MDS code with parameters $[n, n - 2s - \deg((g_1)_0) + 1]$.

Proof. If we take $G = (n-2)P_{\infty}$, $A = 2E + (g_1)_0$ for some divisor E and $B = (g_2)_0 + (n-2(s-1) - \deg(g_1) - \deg(g_2))P_{\infty}$, then plugging G, A, B, (h') into (2), we get

$$\begin{aligned} 2G - A - B - (h') &- (n-2)P_{\infty} \\ &= 2(n-2)P_{\infty} - 2E - (g_1)_0 - (g_2)_0 - (n-2(s-1) - \deg(g_1) - \deg(g_2))P_{\infty} \\ &- 2(f)_0 - (g_1)_0 - (g_2)_0 + (2\deg(f) + \deg(g_1) + \deg(g_2))P_{\infty} - (n-2)P_{\infty} \\ &= 2\left(-E - (g_1)_0 - (g_2)_0 - (f)_0 + (s-1 + \deg(g_1) + \deg(g_2) + \deg(f))P_{\infty}\right) \\ &= \frac{1}{(efg_1g_2)^2}. \end{aligned}$$

We now prove the existence of a place E of degree $s - 1 \ge 0$ such that $E \notin S := \{P_{\infty}\} \cup supp(D) \cup supp((g_1)_0) \cup supp((g_2)_0)$. For s = 1, we take E = 0. Then obviously $E \notin S$. Under the condition $n + \deg(g_1) + \deg(g_2) \le q - 1$, there exists a zero place F of degree one such that $F \notin S$. Take E = (s - 1)F with $s \ge 2$.

A simple calculation gives

[12, Theorem 4] with similar reasoning as 9).

$$G - A - B = ((2s - 2)P_{\infty} - 2E) + (\deg(g_1) + \deg(g_2)P_{\infty} - (g_1)_0 - (g_2)_0) = \frac{1}{(e^2g_1g_2)},$$

which is obviously a principal divisor. The rest follows from Lemma 6.

Corollary 5. Let $q = p^m > 5$ be odd, $n \le q-1$, p|n and (n-1)|(q-1). Then there exist 1-d-hull MDS codes with parameters [n, n-2s+1] and [n, 2s-1] for $1 \le s \le \lfloor \frac{n}{2} \rfloor$.

Proof. Set $h(x) = x^n - x$. The derivative of h(x) is h'(x) = -1. Clearly, h(x) has n simple roots and it gives rise to n distinct places of degree one. Set $(f)_0 = (g_1)_0 = (g_2)_0 = 0$. Then $n + \deg(g_1) + \deg(g_2) = n \le (q - 1)$. By applying Theorem 5, the result follows.

Corollary 6. Let $q = p^m > 5$ be odd with $1 \le r < m$ and r|m. Then there exist 1-d-hull MDS codes with parameters $[p^r, p^r - 2s + 1]$ and $[p^r, 2s - 1]$ for $1 \le s \le \frac{p^r - 1}{2}$.

Proof. Set $h(x) = x^{p^r} - x$. The derivative of h(x) is h'(x) = -1. Clearly, h(x) has $n = p^r$ simple roots and it gives rise to n distinct places of degree one. Set $(f)_0 = (g_1)_0 = (g_2)_0 = 0$. Then $n + \deg(g_1) + \deg(g_2) = p^r \le (q-1)$. By applying Theorem 5, the result follows.

Corollary 7. Let $q = p^m > 5$ be odd with $m \ge 1$ and $n \le (q-2)$. Then

- 1) there exist 1-d-hull MDS codes with parameters [n, n-2s+1] and [n, 2s-1] for $1 \le s \le \lfloor (n-1)/2 \rfloor$,
- 2) there exist 1-d-hull MDS codes with parameters [n, n-2s] and [n, 2s] for n even and $1 \le s \le n/2 1$.

Proof. Set $h(x) = x^n - 1$. The derivative of h(x) is $h'(x) = nx^{n-1}$. Clearly, h(x) has n simple roots and it gives rise to n distinct places of degree one.

Consider the following setting.

1) For n odd, take $(f)_0 = \frac{n-1}{2}(x)_0, (g_1)_0 = (g_2)_0 = 0$ and $1 \le s \le \lfloor n/2 \rfloor$. For n even, take $(f)_0 = \frac{n-2}{2}(x)_0, (g_1)_0 = \frac{n-2$ $0, (g_2)_0 = (x)_0$ and $1 \le s \le \lfloor (n-1)/2 \rfloor$. Hence for both cases, $1 \le s \le \lfloor (n-1)/2 \rfloor$. 2) For *n* even, take $(f)_0 = \frac{n-2}{2}(x)_0, (g_1)_0 = (x)_0, (g_2)_0 = 0.$

With the above setting, we get $n + \deg(q_1) + \deg(q_2) \le n + 1 \le (q-1)$. By applying Theorem 5, the result follows.

By considering additive cosets of some \mathbb{F}_p -subspaces of \mathbb{F}_q , we get the following construction.

Corollary 8. Let $q = p^m > 5$ be odd with $m \ge 2$, $r \le m-1$ and r|m. Set $N = (t+1)p^r$ with gcd(p,t+1) = 1 and $1 \le t \le \lfloor \frac{q-1-p'}{2p^r} \rfloor$. Then there exist 1-d-hull MDS codes with parameters [N, N-2s+1] and [N, 2s-1] for $1 \le s \le \lfloor p^r/2 \rfloor$.

Proof. Let $U_0 = \mathbb{F}_{p^r}$ and $U_i = (\beta_i + U_0)_{1 \le i \le t}$ be t nonzero distinct additive cosets of U_0 . Put $U = U_0 \cup \left(\bigcup_{i=1}^t \beta_i + U_0\right)$. Write

$$a(x) = (x^{p^r} - x), b(x) = \prod_{i=0}^t (x - a(\beta_i)), h(x) = b(a(x)),$$

where $\beta_0 = 0$. The derivative of h(x) is h'(x) = b'(a(x))a'(x), and thus $\deg(h') = (\deg(b)-1)\deg(a) = tp^r$ if $\gcd(t+1,p) =$ 1. It is not difficult to check that h(x) has all its N simple roots in U, and it gives rise to N distinct places of degree one. Setting $(f)_0 = 0, (g_1) = 0$ and $(g_2)_0 = (h')_0$, we get $N + \deg(g_1) + \deg(g_2) = (t+1)p^r + tp^r \le q-1$ if $1 \le t \le \lfloor \frac{q-p'-1}{2p^r} \rfloor$. By applying Theorem 5, the result follows.

By considering cosets of the multiplicative subgroup of \mathbb{F}_q^* of order *n*, we get the following construction.

Corollary 9. Let $q = p^m > 5$ be odd with $m \ge 1$ and n | (q-1). Set N = (t+1)n with $1 \le t \le \lfloor \frac{q-n-2}{2n} \rfloor$. Then there exist 1-d-hull MDS codes with parameters as follows:

- 1) [N, n-2s+1] and [N, tn+2s-1] for $1 \le s \le \lfloor (n-1)/2 \rfloor$, $p \not| (t+1)$,
- 2) [N, 2n 2s + 1] and [N, (t 1)n + 2s 1] for $1 \le s \le \lfloor (2n 1)/2 \rfloor$, $p \mid (t + 1)$,
- 3) [N, n-2s] and [N, tn+2s] for n even, $1 \le s \le \lfloor (n-1)/2 \rfloor$, $p \not| (t+1)$,
- 4) [N, 2n-2s] and [N, (t-1)n+2s] for *n* even, $1 \le s \le \lfloor (2n-1)/2 \rfloor$, $p \mid (t+1)$,
- 5) [N, N-2s+1] and [N, 2s-1] for $1 \le s \le \lfloor (n-1)/2 \rfloor$, $p \not| (t+1)$,
- 6) [N, N-2s+1] and [N, 2s-1] for $1 \le s \le \lfloor (2n-1)/2 \rfloor$, $p \mid (t+1)$,
- 7) [N, N-2s] and [N, 2s] for n even, $1 \le s \le \lfloor (n-1)/2 \rfloor$, $p \not| (t+1)$,
- 8) [N, N-2s] and [N, 2s] for *n* even, $1 \le s \le \lfloor (2n-1)/2 \rfloor$, p|(t+1).

Proof. Let U_n be a multiplicative subgroup of \mathbb{F}_q^* of order n. Let $\beta_1 U_n, \ldots, \beta_t U_n$ be t nonzero cosets of U_n . Write

$$h(x) = (x^n - 1) \prod_{\lambda_1 \in \beta_1 U_n} (x - \lambda_1) \cdots \prod_{\lambda_t \in \beta_t U_n} (x - \lambda_t).$$

The derivative of h(x) is given by

$$h'(x) = nx^{n-1} \left(\sum_{i=0}^{t} \prod_{j=0, j \neq i}^{t} (x^n - \beta_j^n) \right),$$

where $\beta_0 = 1$. Clearly, h(x) has N = (t+1)n simple roots, and it gives rise to N distinct places of degree one. Moreover, we have $(h')_0 = (n-1)(x)_0 + (g)_0$ for some $g \in \mathbb{F}_q[x]$ with the degree of g equal to tn if $p \not| (t+1)$ and equal to (t-1)nif p|(t+1).

For the proof of points 1) and 2), we have the following setting.

- (a) If n is odd, then we set $(f)_0 = \frac{n-1}{2}(x)_0, (g_1)_0 = (g)_0, (g_2)_0 = 0.$ (b) If n is even, then we set $(f)_0 = \frac{n-2}{2}(x)_0, (g_1)_0 = (g)_0, (g_2)_0 = (x)_0.$

For the proof of points 3) and 4), we set, for n even, $(f)_0 = \frac{n-2}{2}(x)_0, (g_1)_0 = (x)_0 + (g)_0, (g_2)_0 = 0.$ For the proof of points 5) and 6) we have the following setting

- (a) If n is odd, then we set $(f)_0 = \frac{n-1}{2}(x)_0, (g_1)_0 = 0, (g_2)_0 = (g)_0.$ (b) If n is even, then we set, $(f)_0 = \frac{n-2}{2}(x)_0, (g_1)_0 = 0, (g_2)_0 = (x)_0 + (g)_0.$

For the proof of points 7) and 8), we set, for *n* even, $(f)_0 = \frac{n-2}{2}(x)_0, (g_1)_0 = (x)_0, (g_2)_0 = (g)_0$. With the above setting, we get $N + \deg(g_1) + \deg(g_2) \le N + \deg(g) + 1 \le (t+1)n + tn + 1 \le q-1$ if $1 \le t \le \lfloor \frac{q-n-2}{2n} \rfloor$. By applying Theorem 5, the result follows.

Example 4. Take $q = 3^4$, n = 8 and t = 1. By applying Corollary 9 7) with s = 3, we obtain a 1-d-hull MDS code C_6 with parameters [16, 10, 7], where its generator matrix is given by

Example 5. Take $q = 3^4$, n = 8 and t = 2. By applying Corollary 9.8) with s = 2, we obtain a 1-d-hull MDS code C_7 with parameters [24, 20, 5], where its generator matrix is given by

$$C_{7} = \begin{pmatrix} w_{1}^{2} & w_{1}^{28} & w_{1}^{44} & w_{1}^{77} \\ w_{3}^{38} & w_{3}^{5} & w_{7} & w_{45} \\ w_{64} & w_{62} & w_{76} & w_{79} \\ 2 & w_{31} & w_{49} & w_{29} \\ w_{8} & w_{59} & w_{65} & w_{36} \\ w_{48} & w_{5} & w_{68} & w_{45} \\ w_{23} & w_{44} & w_{68} & w_{69} \\ w_{22} & w_{35} & w_{22} & w_{41} \\ w_{29} & w_{49} & w_{28} & w_{17} \\ u_{20} & w_{34} & w_{41} & w & w_{21} \\ w_{10} & w_{76} & w_{39} & w_{11} \\ w_{10} & w_{76} & w_{39} & w_{11} \\ w_{46} & w_{11} & w_{34} & w_{8} \\ w_{77} & w_{28} & w_{41} & w_{41} \\ w & w_{2}^{2} & w_{7} & w_{14} \\ w_{37} & w_{56} & w_{24} & w_{23} \\ w_{65} & w_{46} & w_{37} & w_{20} \\ w_{64} & w_{33} & w_{19} & w_{68} \\ w_{37} & w_{77} & w_{51} & 1 \\ w_{37} & w_{11} & w_{55} & w_{47} \\ w_{27}^{27} & w_{28} & w_{28} & w_{68} \end{pmatrix}$$

Remark 2. From Corollary 9, one may get longer 1-d-hull MDS codes by considering larger t, that is, $t \ge \lfloor \frac{q-n-2}{2n} \rfloor + 1$. In this situation, the existence of such codes depends on the existence of a zero place F of degree one such that $F \notin I$ $supp(D) \cup supp((h')_0)$, which depends on the number of zeros of the derivative h'(x). For example, applying $q = 3^4, n = 8$ to Corollary 9 7)–8), the value of t lies between 0 and 4, and we get 1-d-hull MDS codes of lengths N = (t+1)n. However, for t = 5, using Magma [3], we can find a zero place F of degree one such that $F \notin supp(D) \cup supp((h')_0)$, and thus we obtain 1-d-hull MDS codes with parameters [48, 46, 3], [48, 44, 5], [48, 42, 7], [48, 40, 9], [48, 38, 11], [48, 36, 13], [48, 34, 15].

V. CONCLUSION

In this paper, we deal with linear codes having one dimensional hull. The hull is defined with respect to Euclidean inner product, and we construct families of 1-d-hull MDS codes from algebraic geometry codes of genus zero. For the future work, with the same spirit, it is worth considering the hull with respect to Hermitian inner product on the one hand, and consider codes from higher genus and with higher dimensional hull on the other hand.

REFERENCES

- [1] E. F. Assmus, Jr and J. D. Key, "Affine and projective planes," Discrete Math. vol. 83, pp. 161-187, 1990.
- [2] S. Ball, "On sets of vectors of a finite space in which every subset of basis size is a basis," J. Eur. Soc. 14, pp. 733-748, 2012.
- [3] W. Bosma and J. Cannon, Handbook of Magma Functions, Sydney, 1995.
- [4] C. Carlet and 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. 10(1), pp.131-150, 2016.
- [5] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya and P. Solé, "On linear complementary pairs of codes," IEEE Trans. Inf. Theory, 64(10), pp. 6583-6589, 2018.
- [6] C. Carlet, C. Li and S. Mesnager, "Linear codes with small hulls in semi-primitive case," Des. Codes Cryptogr. https://doi.org/10.1007/s10623-019-00663-4
- [7] C. Carlet, S. Mesnager, C. Tang, Y. Qi and R. Pellikaan, "Linear codes over \mathbb{F}_q are equivalent to LCD codes for q > 3," *IEEE Trans. Inf. Theory*, 64(4), pp. 3010-3017, 2018.
- [8] C. Carlet C, S. Mesnager, C. Tang and Y. Qi, "New characterization and parametrization of LCD codes," IEEE Trans. Inf. Theory, 65(1), pp. 39-49, 2019.
- [9] C. Carlet, S. Mesnager, C. Tang and Y. Qi, "Euclidean and Hermitian LCD MDS codes," Des. Codes Cryptogr. 86, pp. 2605–2618, 2018.
- [10] C. Carlet, S. Mesnager, C. Tang and Y. Qi, "On σ -LCD codes," *IEEE Trans. Inf. Theory*, 65(3), pp. 1694–1704, 2019.
- [11] B. Chen and H. Liu, "New constructions of MDS codes with complementary duals," IEEE Trans. Inf. Theory, 64(8), pp. 5776–5782, 2018.
- [12] W. Fang and F. Fu, "New Constructions of MDS Euclidean Self-dual Codes from GRS Codes and Extended GRS Codes," IEEE Trans. Inform. Theory, vol. 65(9), pp. 5574-5579, 2019.
- [13] M. Grassl and T. A. Gulliver, "On Self-Dual MDS Codes" *ISIT 2008*, Toronto, Canada, July 6 –11, 2008 [14] K. Guenda, "New MDS self-dual codes over finite fields," *Des. Codes Cryptogr.* 62, pp. 31–42, 2012.
- [15] L. Jin, "Construction of MDS codes with complementary duals," IEEE Trans. Inf. Theory, 63(5), pp. 2843-2847, 2017.
- [16] L. Jin and P. Beelen, "Explicit MDS Codes With Complementary Duals," IEEE Trans. Inf. Theory, 64(11), pp. 7188 –7193, 2018.

- [17] L. Jin and C. Xing, "New MDS self-dual codes from generalized Reed-Solomon codes," IEEE Trans. Inform. Theory, vol. 63(3), pp. 1434-1438, 2017.
- [18] J. Leon, "Computing automorphism groups of error-correcting codes," IEEE Trans. Inf. Theory, 28(3), pp. 496-511, 1982.
- [19] J. Leon, "Permutation group algorithms based on partition, I: Theory and algorithms," J. Symb. Comput. 12, pp. 533-583, 1991.
- [20] C. Li, C. Ding and S. Li, "LCD cyclic codes over finite fields," IEEE Trans. Inf. Theory, 63(7), pp. 4344-4356, 2017.
- [21] S. Li, C. Li, C. Ding and H. Liu, "Two Families of LCD BCH codes," IEEE Trans. Inf. Theory, 63(9), pp. 5699-5717, 2017.
- [22] C. Li and P. Zeng, "Constructions of linear codes with one-dimensional hull," IEEETrans. Inf. Theory, 65 (3), pp. 1668–1676, 2019.
- [23] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North Holland, 1977.
- [24] J. L. Massey, "Linear codes with complementary duals," Discret. Math.106(107),337-342 (1992).
- [25] S. Mesnager, C. Tang and Y. Qi, "Complementary dual algebraic geometry codes," IEEE Trans. Inf. Theory, 64(4), pp. 2390-2397, 2018.
- [26] E. Sangwisut, S. Jitman, S. Ling, and P. Udomkavanich, "Hulls of cyclic and negacyclic codes over finite fields," Finite Fields Appl. 33, pp. 232-257, 2015.
- [27] N. Sendrier, "On the dimension of the hull," SIAM J. Discret. Math. 10(2), pp. 282-293, 1997.
- [28] N. Sendrier, "Finding the permutation between equivalent codes: the support splitting algorithm," IEEE Trans. Inf. Theory, 46(4), pp. 1193–1203, 2000.
- [29] X. Shi, Q. Yue and S. Yang, "New LCD MDS codes constructed from generalized Reed-Solomon codes," J. Algebra Appl. 18, 1950150, 2018.
- [30] G. Skersys, "The average dimension of the hull of cyclic codes," *Discret. Appl. Math.* 128(1), pp. 275–292, 2003.
 [31] Lin Sok, "Explicit constructions of MDS self-dual codes," *IEEE Transactions on Information Theory*, vol. 66(6), pp. 3603–3615, 2020, doi:10.1109/TIT.2019.2954877
- [32] Lin Sok, "New families of self-dual codes," https://arxiv.org/abs/2005.00726
- [33] H. Stichtenoth, "Algebraic function fields and codes," Springer, 2008.
- [34] H. Tong and X. Wang, "New MDS Euclidean and Hermitian self-dual codes over finite fields," Adv. in Pure Math. vol. 7, pp. 325-333, 2017.
- [35] H. Yan, "A note on the constructions of MDS self-dual codes," Cryptogr. Commun. 11, pp. 259–268, 2019. https://doi.org/10.1007/s12095-018-0288-3
- [36] H. Yan, H. Liu, C. Li and S. Yang, "Parameters of LCD BCH codes with two lengths," Adv. Math. Commun. 12(3), pp. 579–594, 2018.
- [37] X. Yang and J. L. Massey, "The condition for a cyclic code to have a complementary dual," Discret. Math. 126(1-3), pp. 391-393, 1994.