DTU Library

Explicit MDS Codes with Complementary Duals

Beelen, Peter; Jin, Lingfei

Explicit MDS Codes with Complementary Duals

Peter Beelen and Lingfei Jin

Abstract—**In 1964, Massey introduced a class of codes with complementary duals which are called Linear Complimentary Dual (LCD for short) codes. He showed that LCD codes have applications in communication system, side-channel attack (SCA) and so on. LCD codes have been extensively studied in literature. On the other hand, MDS codes form an optimal family of classical codes which have wide applications in both theory and practice. The main purpose of this paper is to give an explicit construction of several classes of LCD MDS codes, using tools from algebraic function fields. We exemplify this construction and obtain several classes of explicit LCD MDS codes for the odd characteristic case.**

Index Terms—**Generalized Reed-Solomon codes, MDS codes, Linear complementary dual, Algebraic geometry codes.**

I. INTRODUCTION

Linear Complementary Dual (LCD) cyclic codes over finite fields were first introduced and studied by Massey in 1964 and they were called reversible codes in [11]. LCD codes have been used in many applications. Besides the applications in communication systems, data storage, Carlet and Guilley [2] showed that LCD codes can be used against side-channel attack (SCA). It was shown that the distance of a code with linear complementary dual represents the security degree against SCA. Hence, for application in

Peter Beelen is with the Department of applied Mathematics and Computer Science, Technical University of Denmark, Kgs. Lyngby 2800, Denmark. *email:* pabe@dtu.dk.

Lingfei Jin is with Shanghai Key Laboratory of Intelligent Information Processing, School of Computer Science, Fudan University, Shanghai 200433, China. She is also with State Key Laboratory Cryptology, P.O. Box5159, Beijing, 100878, China. *email:* lfjin@fudan.edu.cn.

SCA, larger minimum distance is preferred. MDS codes form an optimal family of classical codes in the sense that the minimum distance achieves the Singleton bound.

In [12], Massey showed that there exist asymptotically good LCD codes by establishing a relationship between LCD codes and linear codes and raised a question on whether LCD codes can achieve the Gilbert-Varshamov bound. Later, Sendrier showed that LCD codes meet the asymptotic Gilbert-Varshamov bound using the hull dimension spectra of linear codes [16]. In the literature, LCD codes have been studied extensively and many results and properties for LCD cyclic codes were found [6], [7], [10], [14], [19], [13], [20]. In [8], the problem of constructing LCD MDS codes over finite fields of even characteristic was solved. For the case where the field characteristic is odd, several results were presented in [5], [8], [13], [18]. After this work was completed, we became aware that there is a contemporaneous paper on LCD MDS codes by Carlet et al. [3]. A few days later, it was further showed by them that any linear code is equivalent to an LCD code [4]. As a result, the problem of classifying LCD MDS codes was settled completely in [3], [4]. While the landmark result in [3] cleverly employs techniques from linear algebra, the current work uses the language of function fields and algebraic geometry codes. This enables us to describe and obtain some LCD MDS codes in a very different way. Because of this, we feel that the current work is still of independent interest and may facilitate future investigations of (some) LCD MDS codes, since the full machinery of function fields is available for these codes. We explicitly construct several classes of LCD MDS codes over finite fields of odd characteristic. The algebraic geometry framework gives rise to a finer analysis as to when a generalized Reed-Solomon code is an LCD code as well. Summarizing, we

obtain the following result.

Theorem I.1 *Let $q = p^r$ for an odd prime power q. Then there exist explicit q-ary $[n,k]$-LCD MDS codes for the following ranges of n and k.*

(1) *Set $n = p^t$, with $1 \le t < r$ and $0 \le k \le p^t$ (see Construction III.7 (i)).*

(2) *Set $n < q$ a positive integer such that $p|n$ and $(n-1)|(q-1)$ and $0 \le k \le n$ (see Construction III.7 (ii)).*

(3) *Set $n = p\ell$, with ℓ a divisor of $q-1$ such that $p\ell < q$. If ℓ is even, then $k = 2\ell - 2m$ for any m satisfying $0 \le m \le \ell - 1$. If ℓ is odd, then $k = 2\ell - 2m$ for any m such that $0 \le m \le \ell$ (see Construction III.8).*

(4) *Suppose that $q \ge 5$ is an odd square and let $n < q$ such that $n-1$ is an odd divisor of $q-1$. Then $k = n - 2m$ for any m such that $0 \le m \le n/2$ (see Construction III.9).*

(5) *Set n to be a divisor of $(q-1)/2$. If n is even (resp. odd) $k = n - 2m$ (resp. $k = n - 2m - 1$) for any m such that $1 \le m \le n/2$ (see Construction III.10).*

(6) *Let $r > 1$ and write $N_t = (p^t - 1)/(p - 1)$. Then we set $n = pN_{r-1}$ and k any integer such that $0 \le k \le pN_{r-1}$ (see Construction III.11).*

(7) *Let $t < r$ and choose $1 \le d \le p^{r-t}$ such that $\gcd(d,p) = 1$. Then we can set $n = dp^t$ and $k = dp^t - 2m$ for any m such that $2 \le m \le p^t/2$ (see Construction III.12).*

Remark I.2 (i) Note that part (1) of Theorem I.1 was obtained in [5, Theorem 3.5] using generalized Reed-Solomon codes as well. The parameters in part (5) of Theorem I.1 were also obtained in [18, Theorem 9], though using a different construction involving negacyclic codes. Finally, as mentioned before, in [3] linear algebra techniques were used to construct LCD MDS codes for all feasible parameters, hence also the above.

(ii) The paper [13] presented a construction of LCD algebraic geometry codes from arbitrary curves. Some strict conditions were proposed in [13] in order to obtain LCD algebraic geometry codes. In our paper, we make use of good properties of rational function fields to get LCD algebraic geometry codes under the conditions that are much easier to satisfy.

The paper is organized as follows. We first provide the relevant backgrounds on rational function fields and algebraic geometry codes in Section II. In Section III, we consider the construction of LCD MDS codes from algebraic geometry codes over the rational function field. Sufficient conditions are given for two algebraic geometry codes to be disjoint. This gives rise to Theorem III.2 describing how to construct LCD MDS codes. We then give several constructions that provide the parameters mentioned in Theorem I.1.

II. PRELIMINARIES

A. LCD MDS codes

Throughout this paper, denote by $\mathbb{F}_q$ the finite field of q elements with characteristic p. We define the Euclidean inner product of two vectors $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$ of $\mathbb{F}_q^n$ by $\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^n u_i v_i$. A q-ary linear code C of length n is a subspace of $\mathbb{F}_q^n$. The dual code of C is defined by $C^\perp = \{\mathbf{x} \in \mathbb{F}_q^n : \ \mathbf{x} \cdot \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C\}$. C is called *linear complementary dual* (LCD for short) if $C \cap C^\perp = \{\mathbf{0}\}$.

A linear code with length n, dimension k and minimum distance d is called *maximum distance separable* (MDS for short) if $k + d = n + 1$. In this article we study codes that are both LCD and MDS, that is to say, LCD MDS codes.

B. Rational function field

In this subsection, we briefly review some basic results on function field (in particular, on rational function field). For the details on the theory of function field, the reader may refer to the book [17].

Denote by $\mathcal{F}$ the rational function field $\mathbb{F}_q(x)$ with a transcendental element x over $\mathbb{F}_q$. For an element $\alpha \in \mathbb{F}_q$, the zero place of $x - \alpha$ is denoted by P_α and its pole place by P_∞. These are all rational places (or places of degree 1). Furthermore, every place $R \ne P_\infty$ corresponds to a monic irreducible polynomial $r(x) \in \mathbb{F}_q[x]$. The degree of R, denoted by $\deg(R)$, is defined to be the degree of $r(x)$. Let $\mathbb{P}_\mathcal{F}$ denote the set of places of $\mathcal{F}$.

A divisor G of $\mathcal{F}$ is a formal sum $\sum_{R \in \mathbb{P}_{\mathcal{F}}} m_R R$ with only finitely many nonzero m_R. The support of G is defined to be $\{R \in \mathbb{P}_{\mathcal{F}} : m_R \neq 0\}$. The degree of G is defined to be $\sum_{R \in \mathbb{P}_{\mathcal{F}}} m_R \deg(R)$. A divisor $G = \sum_{R \in \mathbb{P}_{\mathcal{F}}} m_R R$ is said to be bigger than or equal to other divisor $D = \sum_{R \in \mathbb{P}_{\mathcal{F}}} n_R R$ if $m_R \geq n_R$ for all $R \in \mathbb{P}_{\mathcal{F}}$. A divisor $G = \sum_{R \in \mathbb{P}_{\mathcal{F}}} m_R R$ is said to be effective, denoted by $G \geq 0$ if $m_P \geq 0$ for all $R \in \mathbb{P}_{\mathcal{F}}$. For two divisors $G = \sum_{R \in \mathbb{P}_{\mathcal{F}}} m_R R$ and $D = \sum_{R \in \mathbb{P}_{\mathcal{F}}} n_R R$, we define

$$G \vee D := \sum_{R \in \mathbb{P}_{\mathcal{F}}} \max\{m_R, n_R\} R,$$

$$G \wedge D := \sum_{R \in \mathbb{P}_{\mathcal{F}}} \min\{m_R, n_R\} R.$$

It is clear that

$$\deg(G \wedge D) + \deg(G \vee D) = \deg(G) + \deg(D).$$

Assume that a nonzero polynomial $f(x) \in \mathbb{F}_q[x]$ has the canonical factorization $\alpha \prod_{i=1}^{t} r_i(x)^{e_i}$ with $\alpha \in \mathbb{F}_q^*$ and pairwise distinct monic irreducible polynomials $r_i(s)$, the principal divisor (f) of $f(x)$ is $\sum_{i=1}^{t} e_i \deg(R_i) - \deg(f) P_\infty$, where R_i are places corresponding to $r_i(x)$. Now for a rational function $f(x)/g(x) \in \mathcal{F}$ with $g(x) \neq 0$ and $f(x) \neq 0$, the principal divisor (f/g) of $f(x)/g(x)$ is defined to be $(f) - (g)$. For a nonzero function $u \in \mathcal{F}$, we write $(u) = \sum_{P \in \mathsf{P}} m_P P - \sum_{R \in \mathsf{R}} m_R R$, where P and R are two disjoint subsets of $\mathbb{P}_{\mathcal{F}}$ and $m_P > 0$, $m_R > 0$ for all $P \in \mathsf{P}$ and $R \in \mathsf{R}$. The divisors $\sum_{P \in \mathsf{P}} m_P P$ (denoted by $(u)_0$) and $\sum_{R \in \mathsf{R}} m_R R$ (denoted by $(u)_\infty$) are called zero divisor and pole divisor of (u), respectively. It is well known that $\deg((u)_0) = \deg((u)_\infty)$. In particular any principal divisor has degree zero. For the rational function field $\mathcal{F}$ the converse holds: for any divisor G of degree zero, one can find a function $y \in \mathcal{F}$ such that $(y) = G$.

For a divisor G, we define the Riemann-Roch space

$$\mathcal{L}(G) := \{u \in \mathcal{F} \setminus \{0\} : (u) + G \geq 0\} \cup \{0\}.$$

Then $\mathcal{L}(G)$ is an $\mathbb{F}_q$-subspace of dimension $\deg(G) + 1$ for any divisor of nonnegative degree. If for example $G = mP_\infty$, then $\mathcal{L}(G)$ is the

$(m + 1)$-dimensional space of polynomials of degree at most m. It is straightforward to verify that

$$\mathcal{L}(G) \cap \mathcal{L}(H) = \mathcal{L}(G \wedge H) \text{ and}$$

$$\mathcal{L}(G) + \mathcal{L}(H) \subseteq \mathcal{L}(G \vee H).$$

C. Algebraic geometry codes on the rational function field

Let us first define generalized Reed-Solomon codes. Let $\mathbf{a} = (\alpha_1, \ldots, \alpha_n)$ with $\alpha_1, \ldots, \alpha_n$ being n distinct elements of $\mathbb{F}_q$. Let $\mathbf{v} = (v_1, \ldots, v_n) \in (\mathbb{F}_q^*)^n$ be a vector. For $1 \leq k \leq n$, we define

$$\mathsf{GRS}_k(\mathbf{a}, \mathbf{v}) := \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) : $$
$$f(x) \in \mathbb{F}_q[x], \deg(f) \leq k - 1\}. \quad (1)$$

$\mathsf{GRS}_k(\mathbf{a}, \mathbf{v})$ is called a generalized Reed-Solomon code. It is an $[n, k]$-MDS code over $\mathbb{F}_q$.

For convenience, we write $P_i := P_{\alpha_i}$ and let D be the divisor $\sum_{i=1}^{n} P_i$. Further let G be a divisor such that $\mathrm{Supp}(D) \cap \mathrm{Supp}(G) = \emptyset$. Define the following functional algebraic geometry code

$$C_L(D, G) := \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}.$$

It is easy to see that $C_L(D, (k-1)P_\infty)$ is the same as $\mathsf{GRS}_k(\mathbf{a}, \mathbf{v})$ with $\mathbf{v} = (1, \ldots, 1)$. More generally [17, Proposition 2.3.3] implies the following lemma.

Lemma II.1 *If* $1 \leq k \leq n$ *and* G *is a divisor such that* $\deg(G) = k - 1$ *and* $\mathrm{Supp}(G) \cap \mathrm{Supp}(D) = \emptyset$, *then* $C_L(D, G)$ *is equal to the generalized Reed-Solomon code* $\mathsf{GRS}_k(\mathbf{a}, \mathbf{u})$ *for some* $\mathbf{u} \in (\mathbb{F}_q^*)^n$. *Conversely, any generalized Reed-Solomon code* $\mathsf{GRS}_k(\mathbf{a}, \mathbf{v})$ *can be realized as a functional code* $C_L(D, H)$ *for some divisor* H *of degree* $k-1$ *with* $\mathrm{Supp}(H) \cap \mathrm{Supp}(D) = \emptyset$.

To define the dual code of an algebraic geometry code, we need to introduce differentials. For a place R corresponding to a monic irreducible polynomial $r(x) \in \mathbb{F}_q[x]$ and a nonzero polynomial $f(x) \in \mathbb{F}_q[x]$, we denote k by $\nu_R(f)$, where $r(x)^k \| f(x)$. This evaluation can be extended to any nonzero function $f(x)/g(x) \in \mathcal{F}$ with $f(x), g(x) \in \mathbb{F}_q[x]$ by defining $\nu_R(f/g) = \nu_R(f) - \nu_R(g)$. In particular, we set $\nu_R(0) = +\infty$.

If R is the place P_∞, we define $\nu_{P_\infty}(f/g) = \deg(g) - \deg(f)$.

The differential space of $\mathcal{F}$ is defined to be

$$\Omega_\mathcal{F} := \{fdx : f \in \mathcal{F}\}.$$

This is a one-dimensional space over $\mathcal{F}$. For any place $R \neq P_\infty$, we define $\nu_R(fdx) = \nu_R(f)$. Furthermore, we define $\nu_{P_\infty}(fdx) = \nu_{P_\infty}(f) - 2$. For a nonzero function f, the divisor $(fdx) = \sum_{R \in \mathbb{P}_\mathcal{F}} \nu_R(fdx)R$ is called a canonical divisor. It is clear that a canonical divisor has degree -2.

For a divisor G, we define the space

$$\Omega(G) := \{\omega \in \Omega_\mathcal{F} \setminus \{0\} : (\omega) \geq G\} \cup \{0\}.$$

Then $\Omega(G)$ is an $\mathbb{F}_q$-subspace of $\Omega_\mathcal{F}$ of dimension $-\deg(G) - 1$ if $\deg(G) \leq -2$. For an element $\alpha \in \mathbb{F}_q$ and a function f with $\nu_{P_\alpha}(f) \geq -1$, we can write $f = a_{-1}/(x-\alpha) + a_0 + a_1(x-\alpha) + \dots$. The residue of fdx, denoted by $\mathrm{res}_{P_\alpha}(fdx)$, is thus defined to be a_{-1}.

As before, let $D = \sum_{i=1}^n P_i$. For a divisor G with $\mathrm{Supp}(D) \cap \mathrm{Supp}(G) = \emptyset$, the differential algebraic geometry code is defined as follow

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

The following lemma can be found in [17, Theorem 2.2.8 and Proposition 2.2.10].

Lemma II.2 *Let $D = \sum_{i=1}^n P_{\alpha_i}$. For a divisor G with $\mathrm{Supp}(D) \cap \mathrm{Supp}(G) = \emptyset$, we have the following.*

(i) *The dual code of $C_L(D,G)$ is $C_\Omega(D,G)$.*

(ii) *If there exists a differential η such that $\nu_{P_i}(\eta) = -1$ and $\mathrm{res}_{P_{\alpha_i}}(\eta) = 1$ for all $1 \leq i \leq n$. Then $C_\Omega(D,G) = C_L(D, D - G + (\eta))$.*

In [17, Lem. 2.3.6] a differential satisfying the conditions in II.2(ii) is constructed explicitly. Before stating this construction, it is convenient to define

$$g(x) := \prod_{i=1}^n (x - \alpha_i),$$

$$z(x) := \frac{dg}{dx} = \sum_{i=1}^n \prod_{j=1: j \neq i}^n (x - \alpha_j).$$

A first property of the function $z(x)$ is given in the following lemma.

Lemma II.3 *Let $n \leq q$ and let $\alpha_1, \dots, \alpha_n$ be distinct elements of $\mathbb{F}_q$ and define $z(x)$ as above. Then*

$$\deg z(x) = \begin{cases} n-1 & \text{if } p \nmid n, \\ n-2 & \text{if } p \mid n \text{ and } \sum_{i=1}^n \alpha_i \neq 0. \\ < n-2 & \text{otherwise} \end{cases}$$

Moreover, $z(\alpha_i) \neq 0$ for all i.

Proof: Since $z(x) = \frac{dg}{dx}$, we see that $z(x) = nz(x)^{n-1} - (n-1)(\sum_i \alpha_i)z(x)^{n-2} + \cdots$. The first part of the lemma now follows. The final statement follows, since α_i is a simple root of $g(x)$ for all i and hence not a zero of $z(x)$. ∎

With this notation, the construction in [17, Lem. 2.3.6] can be paraphrased as follows. Note that from now on we denote $z(x)$ by z.

Lemma II.4 *Let $\alpha_1, \dots, \alpha_n$ be distinct elements of $\mathbb{F}_q$, and let z be as in Lemma II.3. Then the differential*

$$\omega_z := \left(\sum_{i=1}^n \frac{1}{x - \alpha_i}\right) dx = \frac{z}{(x-\alpha_1) \cdots (x-\alpha_n)} dx$$

has divisor

$$W_z := (z) - D + (n-2)P_\infty.$$

Moreover $\mathrm{res}_{P_i}(\omega_z) = 1$ for all i between 1 and n.

It will be convenient to write Z for the divisor of zeroes of z. With this notation, we have $(z) = Z - (\deg(z))P_\infty$. Lemma II.3 implies that $\deg(Z) = \deg(z) \leq n - 1$ as well as that $\mathrm{Supp}(Z) \cap \mathrm{Supp}(D) = \emptyset$. Combining Lemmas II.2 and II.4, we obtain the following result.

Lemma II.5 *Let D, G be as defined in Lemma II.4. Then the dual of $C_L(D,G)$ is $C_L(D, (z) - G + (n-2)P_\infty)$.*

Using the divisor Z, we may also write that $C_L^\perp(D,G) = C_L(D, Z - G + (n - 2 - \deg(z))P_\infty)$.

III. CONSTRUCTION OF LCD MDS CODES

In this section we construct several classes of LCD MDS codes. We first give a sufficient condition under which two functional algebraic geometry codes are disjoint.

Lemma III.1 *Assume that A, B are two positive divisors such that*

(i) $\mathrm{Supp}(A)$, $\mathrm{Supp}(B)$, $\mathrm{Supp}(D)$ *and* $\mathrm{Supp}(H)$ *are pairwise disjoint;*

(ii) $\deg(D) = n > \deg(H)$ *and* $\deg(A) + \deg(B) > \deg(H)$.

Further let $w \in \mathbb{F}_q(x)$ be a function satisfying $v_{P_{\alpha_i}}(w) = 0$ for all i between 1 and n. Then the codes $C_L(D, H - A + (w))$ and $C_L(D, H - B + (w))$ are disjoint.

Proof: Write $v_i = w^{-1}(P_i)$. Then for all i we have $v_i \neq 0$. Now assume that $\mathbf{c} \in C_L(D, H - A + (w)) \cap C_L(D, H - B + (w))$. Then there exist $f_1 \in \mathcal{L}(H - A)$ and $f_2 \in \mathcal{L}(H - B)$ such that $(v_1 f_1(P_1), \ldots, v_n f_1(P_n)) = \mathbf{c} = (v_1 f_2(P_1), \ldots, v_n f_2(P_n))$. Since for all i we have $v_i \neq 0$ and $\mathrm{Supp}(D) \cap \mathrm{Supp}(H) = \emptyset$, we have $f_1 - f_2 \in L(H - D)$. Hence $f_1 - f_2 = 0$, since $\deg(H) < n$. Thus, $f_1 = f_2 \in \mathcal{L}(H - A) \cap \mathcal{L}(H - B) = \mathcal{L}((H - A) \wedge (H - B)) = \mathcal{L}(H - A - B) = \{0\}$. Here we used the assumption that $\deg(A) + \deg(B) > \deg(H)$ in the last equality. ∎

Now we are going to construct LCD MDS codes. The idea is to use Lemma III.1 for suitably chosen divisors H, A and B and a function y such that $C_L^\perp(D, H - A + (y)) = C_L(D, H - B + (y))$.

Theorem III.2 *Let $D = \sum_{i=1}^{n} P_i$, H a divisor and A, B two positive divisors such that:*

(i) $\mathrm{Supp}(A)$, $\mathrm{Supp}(B)$, $\mathrm{Supp}(D)$ *and* $\mathrm{Supp}(H)$ *are pairwise disjoint;*

(ii) $\deg(H) = n - 1$ *and*

(iii) $2H - A - B - (z) - (n - 2)P_\infty$ *equals (y) for some element $y \in \mathbb{F}_q(x)$ such that $y(P_i)$ are squares in $\mathbb{F}_q^*$ for all $1 \leq i \leq n$.*

Then for any $w \in \mathbb{F}_q(x)$ such that $w(P_i)^{-2} = y(P_i)$ for all $1 \leq i \leq n$, the code $C_L(D, H - A + (w))$ is an $[n, n - \deg(A)]$ LCD MDS code.

Proof: First of all, note that the assumptions (ii) and (iii) imply that $\deg(A) + \deg(B) = n$, since any principal divisor has degree zero. Further note that the support of $2H - A - B - (z) - (n - 2)P_\infty$ is disjoint with $\mathrm{Supp}(D)$.

By Lemma III.1, we know that $C_L(D, H - A + (w))$ and $C_L(D, H - B + (w))$ are disjoint. It is now sufficient to show that the dual of $C_L(D, H -$

$A + (w))$ is exactly $C_L(D, H - B + (w))$. By Lemmas II.5, the dual of $C_L(D, H - A + (w))$ is

$$
\begin{aligned}
& C_L(D, -H + A - (w) + (z) + (n - 2)P_\infty) \\
& = C_L(D, H - B - (w) - (y)) \\
& = C_L(D, H - B + (w) - (yw^2)).
\end{aligned}
$$

We claim that $C_L(D, H - B + (w) - (yw^2)) = C_L(D, H - B + (w))$. There is a natural isomorphism of vector spaces between the Riemann–Roch spaces $L(H - B + (w) - (yw^2))$ and $L(H - B + (w))$ sending $f \in L(H - B + (w) - (yw^2))$ to $f/(yw^2) \in L(H - B + (w))$. This map induces an isomorphism of codes $\phi : C_L(D, H - B + (w) - (yw^2)) \to C_L(D, H - B + (w))$ defined by

$$
\phi(f(P_1), \ldots, f(P_n)) = \left(\frac{f}{yw^2}(P_1), \ldots, \frac{f}{yw^2}(P_n) \right).
$$

However, since $(yw^2)(P_i) = 1$ for all $1 \leq i \leq n$, we have $\phi(f(P_1), \ldots, f(P_n)) = (f(P_1), \ldots, f(P_n))$. Hence $C_L(D, H - B + (w) - (yw^2)) = C_L(D, H - B + (w))$ as claimed. This completes the proof. ∎

Note that by the assumption that $y(P_i)$ is a non-zero square for all i, an element w satisfying $w(P_i)^{-2} = y(P_i)$ exists. Moreover, the code $C_L(D, H - A + (w))$ does not depend on the choice of w.

By setting $H = (n - 1)P_\infty$ in Theorem III.2, we obtain the main result of [8] as a corollary.

Corollary III.3 *Let $a(x), b(x)$ be two co-prime polynomials. Let A, B be the zero divisors of $a(x)$ and $b(x)$, respectively. Assume that*

(i) $\mathrm{Supp}(D)$ *is disjoint with both $\mathrm{Supp}(A)$ and $\mathrm{Supp}(B)$;*

(ii) $\deg(a(x)) + \deg(b(x)) = n$ *and*

(iii) $(abz)(P_i)$ *are square elements of $\mathbb{F}_q^*$ for all $1 \leq i \leq n$.*

Then for any element $w \in \mathbb{F}_q(x)$ such that $w(P_i)^2 = (abz)(P_i)$ for all $1 \leq i \leq n$, the code $C_L(D, (n - 1)P_\infty - A + (w))$ is an LCD MDS code.

Proof: In Theorem III.2, set $H = (n - 1)P_\infty$. Then $2H - A - B - (z) - (n - 2)P_\infty$ is the principal divisor of $1/(abz)$. The desired result now follows from Theorem III.2. ∎

One way to make sure that the function y in Theorem III.2 satisfies that $y(P_i)$ is a non-zero

square for all i is by making sure that y itself is a square. This is the main idea behind the following corollary.

Corollary III.4 *Let $m \geq 0$ and $3 \leq n \leq q$. Further, let X and Y be positive divisors such that $Z = 2X + Y$. Finally let Y_1 and Y_2 be disjoint positive divisors such that $Y = Y_1 + Y_2$.*

(i) *There exists a q-ary $[n, n - 2m - \deg(Y_1)]$-LCD MDS code for any $2 \leq m \leq (n - \deg(Y))/2$ or $m = 0$;*

(ii) *If there exists a place P of degree one not in $\mathrm{Supp}(D) \cup \mathrm{Supp}(Y_2) \cup \{P_\infty\}$ and $\deg(Y) \leq n - 2$, then there exists a q-ary $[n, n - 2 - \deg(Y_1)]$-LCD MDS code.*

Proof: First we prove (i). Choose Q to be a place of degree $n - 1$ and set $H = Q$. Since $n \geq 3$, we have $\mathrm{Supp}(H) \cap \mathrm{Supp}(D) = \emptyset$. If $m = 0$, set $K = 0$, which trivially implies that $\mathrm{Supp}(K) \cap \mathrm{Supp}(D) = \emptyset$, $\mathrm{Supp}(K) \cap \mathrm{Supp}(H) = \emptyset$ and $\mathrm{Supp}(K) \cap \mathrm{Supp}(Y_2) = \emptyset$. If $m \geq 2$, we set $K = R$, with R a place of degree m. Since $m \neq 1$, we have $\mathrm{Supp}(K) \cap \mathrm{Supp}(D) = \emptyset$. Moreover, since $n \geq 3$, we have $m \leq n/2 < n - 1$, whence $\mathrm{Supp}(K) \cap \mathrm{Supp}(H) = \emptyset$. Next, we show that we can choose R such that $R \notin \mathrm{Supp}(Y_2)$. The set $\mathrm{Supp}(Y_2)$ contains at most $\deg(Y_2)/m$ places of degree m. Note that

$$\frac{\deg(Y_2)}{m} \leq \frac{\deg(Z)}{m} \leq \frac{n-1}{m} \leq \frac{q-1}{m}.$$

On the other hand, the number of places of degree m is at least $(q^m - q^{\lfloor m/2 \rfloor + 1})/m$ for $m > 2$ and equal to $(q^2 - q)/2$ for $m = 2$. Hence, we see that we can choose the place R of degree m such that $R \notin \mathrm{Supp}(Y_2)$.

Now with such a choice of R, let $A = 2K + Y_1$ and $B = Y_2 + (n - 2m - \deg(Y))P_\infty$. Then

$$2H - A - B - (z) - (n-2)P_\infty$$
$$= 2(H - K - X - Y - (n - 1 - m$$
$$- \deg(X) - \deg(Y))P_\infty)$$

is equal to (f^2) for some $f \in \mathbb{F}_q(x)$. The desired result follows from Theorem III.2 since $y(P_i) = f(P_i)^2$ are non-zero square elements of $\mathbb{F}_q$ for all $1 \leq i \leq n$.

The proof of (ii) is similar. We choose $K = P$. ∎

Note that if $n < q$ and Y_2 is chosen to be 0, the place P in part (ii) of the theorem is guaranteed to exist.

Remark III.5 In characteristic two, the derivative of any polynomial is a square. In particular, the function z is always a square, which implies that $Z = 2X + Y$ for a positive divisor X and $Y = 0$, whence we can choose $Y_1 = Y_2 = 0$. Corollary III.4 then implies that in characteristic two, for any $0 \leq m \leq n/2$ and $3 \leq n \leq q$ there exists an $[n, n-2m]$-LCD MDS code. This result is already contained in [8], where $[n, k]$-LCD MDS codes were found in even characteristic for any $0 \leq n \leq q$ and $0 \leq k \leq n$.

Remark III.6 Suppose q is odd and $n = q$. Then $g = x^q - x$ in our construction, implying that $Z = 0$. Using Corollary III.4 with $X = Y = Y_1 = Y_2 = 0$, we obtain $[q, q - 2m]$-LCD MDS codes for $m = 0$ and $2 \leq m \leq q/2$. Considering the duals of these codes, we obtain $[q, 2m]$ codes for $2 \leq m \leq q/2$. Combined, we see that one can obtain explicit $[q, k]$-LCD MDS codes for nearly all values of k between 0 and q, except $k \in \{2, q - 2\}$.

Because of the above two remarks, our main interest is to construct explicit $[n, k]$-LCD MDS codes in case q is odd and $n < q$. We now give several explicit constructions, exemplifying the versatility of Theorem III.2 and its two corollaries.

Construction III.7 Let $q = p^r$ with a prime p and integer $r \geq 1$.

(i) For any integer t with $1 \leq t \leq r$, let V be an $\mathbb{F}_p$-subspace of $\mathbb{F}_q$ of dimension t. Put $g = \prod_{\alpha \in V}(x - \alpha)$. Then $z = \frac{dg}{dx} = \prod_{\alpha \in V \setminus \{0\}} \alpha$ is a nonzero constant. Hence we have $Z = 0$. By Corollary III.4, there exists a q-ary $[p^t, p^t - 2m]$-LCD MDS code for $m = 0$ (which is trivial in this case) or $2 \leq m \leq p^t/2$. If $t < r$, such a code exists for $0 \leq m \leq p^t/2$. Considering dual codes as well, we see that if p is odd and $t < r$, we can construct explicit $[p^t, k]$-LCD MDS codes for any k satisfying $0 \leq k \leq p^t$.

(ii) Let n be a positive integer with $p|n$ and $(n - 1)|(q - 1)$. Put $g(x) = x^n - x$. Then

$g(x)$ has all roots in $\mathbb{F}_q$ and every root is simple. Furthermore, $z = \frac{dg}{dx} = -1$, whence $Z = X = Y = 0$. Using Corollary III.4, we find an explicit q-ary $[n, n-2m]$-LCD MDS code for $m = 0$ and $2 \le m \le n/2$. If $n < q$ and n is odd, we obtain explicit $[n, k]$-LCD MDS codes for any k with $0 \le k \le n$ by considering the previous constructed codes and their duals.

For example, $q = 81$ and $n = 21$. Then one obtains explicit 81-ary $[21, k]$-LCD MDS codes for any $0 \le k \le 21$.

Construction III.8 Let $q = p^r$ with a prime p and integer $r \ge 1$. Let $q - 1 = \ell \cdot d$ and suppose that $p < d$. Further, let U_ℓ be the multiplicative subgroup of $\mathbb{F}_q^*$ of order ℓ and $\beta_1 U_\ell, \ldots, \beta_p U_\ell$ be pairwise distinct cosets. Consider the polynomials $f(x) := \prod_{i=1}^p (x - \beta_i^\ell)$ and $g(x) := f(x^\ell)$. Then $g(x)$ has no multiple roots and $z = \frac{dg}{dx} = \ell x^{\ell-1} \frac{df}{dx}(x^\ell)$. Choosing $\beta_i = \gamma^i$, with γ a primitive element of $\mathbb{F}_q^*$, we have $\sum_{i=1}^p \beta_i^\ell \ne 0$ and $\frac{df}{dx}(P_0) \ne 0$. Hence in this case $\deg(z) = \ell - 1 + \ell(p-2) = \ell(p-1) - 1$ and $Z = (\ell - 1)P_0 + E$ for some positive divisor E of degree $\deg(E) = \ell(p-2)$ with $P_0 \notin \mathrm{Supp}(E)$.

If ℓ is even, we can choose $X = (\ell - 2)/2 P_0$ and $Y = P_0 + E$. Choosing $Y_1 = Y$ and $Y_2 = 0$, we obtain from Corollary III.4 explicit $[p\ell, 2\ell - 1 - 2m]$-LCD MDS codes for $0 \le m \le \ell - 1$. Choosing $Y_1 = E$ and $Y_2 = P_0$, we obtain from Corollary III.4 explicit $[p\ell, 2\ell - 2m]$-LCD MDS codes for $0 \le m \le \ell-1$. Note that the assumption $p < d$ implies that $p\ell \le (d-1)\ell = q-1-\ell \le q-2$. Therefore a place P as in part (ii) of Corollary III.4 exists.

If ℓ is odd, we can choose $X = (\ell - 1)/2 P_0$ and $Y = E$. Choosing $Y_1 = E$ and $Y_2 = 0$, we construct $[p\ell, 2\ell - 2m]$-LCD MDS codes for $0 \le m \le \ell$.

Construction III.9 Let $q \ge 5$ be an odd square. Let $n - 1$ be an odd divisor of $q - 1$ and $n < q$. Then $n - 1 \le (q-1)/2$, i.e., $n \le (q-1)/2 + 1$. Let $g(x) = x^n - x$. Then $g(x)$ has no multiple roots and splits completely in $\mathbb{F}_q$. Furthermore, $z(x) = \frac{dg}{dx} = nx^{n-1} - 1$. Label the roots of $g(x)$ by $\alpha_1, \ldots, \alpha_n$. Then we have $z(\alpha_i) = n - 1$ or

-1 for all $1 \le i \le n$. Since q is a square, we can find $\theta, \delta \in \mathbb{F}_q$ such that $\theta^2 = n - 1$ and $\delta^2 = -1$.

Now for any $1 \le m \le n/2$, choose two distinct elements $\beta, \gamma \in \mathbb{F}_q$ that are not roots of $g(x)$ (this is possible since $n \le (q-1)/2 + 1 \le q - 2$). Put $a(x) = (x - \beta)^{2m}$ and $b(x) = (x - \gamma)^{n-2m}$. Then $(abz)(\alpha)$ is equal to $(\theta(\alpha - \beta)^m (\alpha - \gamma)^{n/2-m})^2$ or $(\delta(\alpha - \beta)^m (\alpha - \gamma)^{n/2-m})^2$ for all roots α of $g(x)$. Thus, by Corollary III.3 we obtain a q-ary $[n, n-2m]$-LCD MDS code for all $m \le n/2$.

Construction III.10 Let q be odd and let n be a divisor of $(q-1)/2$. Let $g(x) = x^n - 1$. Then every root of $g(x)$ is a square element of $\mathbb{F}_q$. It is clear that $g(x)$ has no multiple roots and splits completely in $\mathbb{F}_q$. Furthermore, $z(x) = \frac{dg}{dx} = nx^{n-1}$.

For any $1 \le m \le n/2$, choose two distinct elements $\beta, \gamma \in \mathbb{F}_q$ that are not roots of $g(x)$ (this is possible since $n \le q - 2$). Put

$$(a(x), b(x)) = \begin{cases} (n(x-\beta)^{2m}, (x-\gamma)^{n-2m}) & \text{if } n \text{ is even} \\ (nx(x-\beta)^{2m}, (x-\gamma)^{n-1-2m}) & \text{if } n \text{ is odd} \end{cases}$$

For every root α of $g(x)$, let $\alpha = \alpha_1^2$ for some $\alpha_1 \in \mathbb{F}_q$. Then

$$(abz)(\alpha) = \begin{cases} (n\alpha_1^{n-1}(\alpha-\beta)^m(\alpha-\gamma)^{n/2-m})^2 & \text{if } n \text{ is even} \\ (n\alpha_1^n(\alpha-\beta)^m(\alpha-\gamma)^{(n-1)/2-m})^2 & \text{if } n \text{ is odd} \end{cases}$$

Thus, by Corollary III.3 we obtain a q-ary $[n, n-2m]$-LCD MDS code for even n and a q-ary $[n, n-2m-1]$-LCD MDS code for odd n.

Construction III.11 Let $q = p^r$ for some odd prime power p and integer $r > 1$. Define $N_r := (p^r - 1)/(p-1)$. Further define the polynomial $g = ((x+1)^{N_r} - 1)/x$. Then g is a polynomial of degree $n := N_r - 1 = pN_{r-1}$ with simple roots, all in $\mathbb{F}_q$. A direct computation shows that $z = -x^{p-2}\left(((x+1)^{N_{r-1}} - 1)/x\right)^p$, implying that $\deg(z) = n - 2$. Moreover, we see that $Z = (p-2)P_0 + p\sum_{i=1}^s Q_i$, where $Q_1, \ldots, Q_s$ denote the zeroes of $(x+1)^{N_{r-1}} - 1$ different from P_0. Note that z has all its roots in $\mathbb{F}_{p^{r-1}}$. Since q is odd, we can choose $Y = P_0 + \sum_{i=1}^s Q_i$, which

is a divisor of degree

$$
\begin{aligned}
\deg(Y) &= 1 + \sum_{i=1}^{s} \deg(Q_i) \\
&= 1 + \frac{\deg(Z) - p + 2}{p} \\
&= 1 + \frac{n - p}{p} = N_{r-1}.
\end{aligned}
$$

Choosing $Y_1 = 0$, we obtain using Corollary III.4 a q-ary $[pN_{r-1}, pN_{r-1}-2m]$-LCD MDS code for $0 \le m \le (p^{r-1} - 1)/2$. Note that since z has its roots in $\mathbb{F}_{p^{r-1}}$, there will be a place of degree one, satisfying the conditions in part (ii) of Corollary III.4. Choosing $Y_1 = P_0$, we similarly obtain a q-ary $[pN_{r-1}, pN_{r-1} - 2m - 1]$-LCD MDS code for $0 \le m \le (p^{r-1} - 1)/2$.

Combining these two results, we see that we have obtained an explicit q-ary $[pN_{r-1}, k]$-LCD MDS code for $N_{r-1} - 1 \le k \le pN_{r-1}$. Considering the duals of these codes, we can strengthen this conclusion to the statement that we obtain an explicit q-ary $[pN_{r-1}, k]$-LCD MDS code for $0 \le k \le pN_{r-1}$.

Construction III.12 Suppose $q = p^r$ and let $V \subset \mathbb{F}_q$ be an $\mathbb{F}_p$ vector space of dimension $t < r$. We define $g_V(x) := \prod_{\alpha \in V}(x - \alpha)$. Further let $\alpha_1 + V, \ldots, \alpha_d + V$ be mutually distinct cosets of V in $\mathbb{F}_q$. This property can also be expressed by saying that $g_V(\alpha_1), \ldots, g_V(\alpha_d)$ are mutually distinct. It is clear that $1 \le d \le p^{r-t}$. Now define $f := \prod_{i=1}^{d}(x - g_V(\alpha_i))$ and set $g := f(g_V(x))$. The polynomial g has no multiple roots and its roots are exactly the dp^t elements of $\mathbb{F}_q$ occurring in the cosets $\alpha_1 + V, \ldots, \alpha_d + V$.

We see that $z = \frac{df}{dx}(g_V(x)) \cdot \prod_{\alpha \in V \setminus \{0\}} \alpha$. Hence $\deg(z) = \deg\left(\frac{df}{dx}\right) p^t$. If $\gcd(d, q) = 1$, we can conclude that $\deg(z) = (d - 1)p^t$. Choosing $Y = Z$ and $Y_1 = 0$, we see from Corollary III.4 that if $\gcd(d, p) = 1$, we obtain q-ary $[dp^t, dp^t - 2m]$-LCD MDS codes for $2 \le m \le p^t/2$.

Collecting the results from the explicit constructions given above, Theorem I.1 follows immediately.

IV. Conclusion

In this paper, we use rational function fields to construct AG codes that are LCD MDS in Theorem III.2. We exemplify this construction and obtain several classes of explicit LCD MDS codes for the odd characteristic case. These constructions are summarized in Theorem I.1 Note that the examples are not meant as an exhaustive list and that it is likely possible to obtain more LCD MDS codes from our construction. Though the problem of classifying LCD MDS codes was completely settled in [3], [4], the algebraic geometry framework in our paper provides tools that could be used to carry out a finer analysis as to when a generalized Reed-Solomon code is an LCD code.

V. Acknowledgements

References

[1] T. Aaron Gulliver, J.-L. Kim and Y. Lee, *New MDS and near-MDS self-dual codes,* IEEE Trans. on Inform. Theory 54, 4354-4360, 2008.

[2] 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, 97-105, Springer Verlag, 2014.

[3] C. Carlet, S. Mesnager, C. Tang, and Y. Qi, *Euclidean and Hermitian LCD MDS codes,* https://arxiv.org/abs/1702.08033v2.

[4] C. Carlet, S. Mesnager, C. Tang, and Y. Qi, *Linear codes over $\mathbb{F}_q$ which are equivalent to LCD codes*, https://arxiv.org/abs/1703.04346.

[5] B. C. Chen and H. W. Liu, *New constructions of MDS codes with complementary duals,* arxiv.org/pdf/1702.07831, 2017.

[6] S. T. Dougherty, J.-L. Kim, B. Ozkaya, L. Sok and P. Solé, *The combinatorics of LCD codes: Linear Programming bound and orthogonal matrices,* Int. J. Information and Coding Theory 4, nos. 2-3, 116C128, 2017.

[7] M. Esmaeili and S. Yari, *On complementary-dual quasi-cyclic codes,* Finite Fields and Their Applications 15, 375-386, 2009.

[8] L. F. Jin, *Construction of MDS codes with complementary duals,* IEEE Trans. on Inform. Theory 63, no. 5, 2843-2847, 2017.

[9] J. -L. Kim and Y. Lee, *Euclidean and Hermitian self-dual MDS codes over large finite fields,* J. Combin. Theory Ser. A, 79-95, 2004.

[10] C. Li, C. Ding and S. Li, *LCD cyclic codes over finite fields*, arXiv:1608.02170, 2016.

[11] J. L. Massey, *Reversible codes,* Information and Control 7, no. 3, 369-380, 1964.

[12] J. L. Massey, *Linear codes with complementary duals,* Discrete Math. 106/107, 337-342, 1992.

[13] S. Mesnager, C. Tang and Y. Qi, *Complementary dual algebraic geometry codes*, arXiv:1609.05649v2.

[14] S. K. Muttoo and S. Lal, *A reversible code over GF(q),* Kybernetika 22, 85-91, 1986.

[15] R. Lidl and H. Niederreiter, "Finite fields", Cambridge University Press, 1993.

[16] N. Sendrier, *Linear codes with complementary duals meet the Gilbert-Varshamov bound,* Discrete Mathematics 285, 345-347, 2004.

[17] H. Stichentonth, "Algebraic function fields and codes", Springer, 2008.

[18] M. Sari and M. E. Körŏglu, On MDS negacyclic LCD codes, arXiv:1611.06371, 2016.

[19] K. K. Tzeng and C. R. P. Hartmann, *On the minimum distance of certain reversible cyclic codes,* IEEE Trans. Inform. Theory 16, 644-646, 1970.

[20] X. Yang, J. L. Massey, *The necessary and sufficient condition for a cyclic code to have a complementary dual,* Discrete Math. 126, 391-393, 1994.

Peter Beelen received his Masters degree in Mathematics from the University of Utrecht, The Netherlands, in 1996. In 2001 he received his Ph.D. degree in Mathematics from the Technical University of Eindhoven, The Netherlands. Since October 2004 he has worked at the Technical University of Denmark (DTU). He has been an assistant professor at DTU till January 2007 and an associate professor till August 2014. Since September 2014 he has worked at DTU as professor. His research interests include various aspects of algebra and its applications, notably algebraic curves and algebraic coding theory.

Lingfei Jin received her B.A. degree in mathematics from Hefei University of Technology, China in 2009. In 2013, she received her Ph.D. degree from Nanyang Technological University, Singapore. Currently, she is an associate Professor at the School of Computer Science, Fudan University, China. Her research interests include classical coding theory and quantum coding theory.