Bull. Aust. Math. Soc. **98** (2018), 159–166
doi:10.1017/S0004972718000175

ON LINEAR COMPLEMENTARY DUAL FOUR CIRCULANT CODES

HONGWEI ZHU and MINJIA SHI[✉]

(Received 25 January 2018; accepted 29 January 2018; first published online 29 April 2018)

Abstract

We study linear complementary dual four circulant codes of length $4n$ over $\mathbb{F}_q$ when q is an odd prime power. When $q^\delta + 1$ is divisible by n, we obtain an exact count of linear complementary dual four circulant codes of length $4n$ over $\mathbb{F}_q$. For certain values of n and q and assuming Artin's conjecture for primitive roots, we show that the relative distance of these codes satisfies a modified Gilbert–Varshamov bound.

2010 *Mathematics subject classification*: primary 94B05; secondary 94B15.

Keywords and phrases: four circulant codes, linear complementary dual (LCD) codes, Artin's conjecture, Chinese remainder theorem.

1. Introduction

Linear complementary dual (LCD) codes are linear codes that intersect with their dual trivially. This concept was introduced by Massey [11], motivated by a problem in information theory. Boolean masking, of interest in embedded cryptography, led to a rediscovery of LCD codes in [4]. Self-dual double negacirculant (circulant) codes over finite fields have been studied in [1, 2] and self-dual four negacyclic (circulant) codes over finite fields have been studied in [13, 14]. In these four papers, the authors derive a modified Gilbert–Varshamov bound on the relative distance for the codes, building on exact enumeration results for a given code length and finite field. A natural question is to ask for a modified Gilbert–Varshamov bound on the relative distance for LCD four circulant codes over finite fields.

This paper will give an answer to this question. Section 2 introduces some basic concepts and definitions. Section 3 develops the machinery of the Chinese remainder theorem (CRT) approach to four circulant codes. Section 4 gives the exact enumeration of LCD four circulant codes over finite fields. Section 5 is dedicated to asymptotic bounds on the relative Hamming distance of these codes when their lengths tend to infinity.

This research is supported by the National Natural Science Foundation of China (61672036), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133) and Key Projects of Support Program for Outstanding Young Talents in Colleges and Universities (gxyqZD2016008).

2. Notation and definitions

Let q be a prime power. A *linear code* C of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$. If $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ are two elements of $\mathbb{F}_q^n$, their standard (Euclidean) inner product is $\langle x, y\rangle_E = \sum_{i=1}^n x_i y_i$, where the operation is performed in $\mathbb{F}_q^n$. The Euclidean dual code $C^{\perp_E}$ of C over $\mathbb{F}_q$ is defined by

$$C^{\perp_E} = \{y \in \mathbb{F}_q^n \mid \langle x, y\rangle_E = 0 \text{ for all } x \in C\}.$$

A linear code C of length n over $\mathbb{F}_q$ is called an *LCD code with respect to the Euclidean inner product* if $C \cap C^{\perp_E} = \{0\}$.

Define the conjugate $\overline{a}$ of $a \in \mathbb{F}_q$ by $\overline{a} = a^{\sqrt{q}}$. The Hermitian inner product of x and y in $\mathbb{F}_q^n$ is defined by $\langle x, y\rangle_H = \sum_{i=1}^n x_i \overline{y_i}$. The Hermitian dual code $C^{\perp_H}$ of C over $\mathbb{F}_q$ is defined by

$$C^{\perp_H} = \{y \in \mathbb{F}_q^n \mid \langle x, y\rangle_H = 0 \text{ for all } x \in C\}.$$

A linear code C of length n over $\mathbb{F}_q$ is called an *LCD code with respect to the Hermitian inner product* if $C \cap C^{\perp_H} = \{0\}$.

A matrix A over $\mathbb{F}_q$ is said to be *circulant* if its rows are obtained by successive shifts from the first row. If the rows are obtained by successive negative shifts from the first row, the matrix is said to be *negacirculant*. A code is called a *double circulant* (*negacirculant*) *code* if its generator matrix is of the form

$$(I_n, A),$$

where I_n is the identity matrix of order n and A is a circulant (negacirculant) matrix. In polynomial form this can be written as $(1, a(x))$, where the x-expansion of the polynomial $a(x)$ is the first row of A.

A linear code C is called a *four circulant code* if the code C is generated by

$$\begin{pmatrix} I_n & 0 & A & B \\ 0 & I_n & -B^t & A^t \end{pmatrix},$$

where A, B are circulant matrices and the exponent 't' denotes transposition. This so-called *four circulant construction* was introduced in [3] and revisited in [8]. If $AA^t + BB^t + I_n = 0$, then C is a self-dual code.

From an algebraic perspective, we can view such a code C as an $R[x]/(x^n - 1)$ submodule in $(R[x]/(x^n - 1))^4$, and the generator matrix of C is

$$\begin{pmatrix} 1 & 0 & a(x) & b(x) \\ 0 & 1 & -b'(x) & a'(x) \end{pmatrix},$$

where $a'(x)$, $b'(x)$ are two polynomials of degree less than n, uniquely defined by the conditions $a'(x) = a(x^{n-1}) \bmod (x^n - 1)$, $b'(x) = b(x^{n-1}) \bmod (x^n - 1)$.

Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m \in \mathbb{F}_q[x]$ with $a_m \neq 0$. The *reciprocal polynomial* $f^*(x)$ of $f(x)$ is defined by $f^*(x) = x^m f(1/x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_m$. The polynomial $f(x)$ is a self-reciprocal polynomial if $f(x) = f^*(x)$. (See [9] for more on reciprocal polynomials.)

https://doi.org/10.1017/S0004972718000175 Published online by Cambridge University Press

Denote by T the standard shift operator on $\mathbb{F}_q^n$. A linear code C is said to be a *quasi-cyclic code of index* l if it is invariant under T^l. Obviously, a four circulant code is a quasi-cyclic code of index four.

If $C(n)$ is a family of codes with parameters $[n, k_n, d_n]$ over $\mathbb{F}_q$, the rate ρ and relative distance δ are defined as $\rho = \limsup_{n\to\infty} k_n/n$ and $\delta = \liminf_{n\to\infty} d_n/n$, respectively. A family of codes is called *asymptotically good* if $\rho\delta > 0$.

3. Algebraic structure of four circulant codes

We assume that q is an odd prime power and $\gcd(n, q) = 1$. According to [10], the factorisation of $x^n - 1$ into distinct irreducible polynomials over $\mathbb{F}_q$ takes the form

$$x^n - 1 = \alpha(x-1)\prod_{i=1}^{s} g_i(x)\prod_{j=1}^{t} h_j(x)h_j^*(x),$$

where $\alpha \in \mathbb{F}_q^*$, $g_i(x)$ is a self-reciprocal polynomial with $\deg(g(x)) = 2k_i$ for $1 \le i \le s$, and $h_j^*(x)$ is the reciprocal polynomial of $h_j(x)$ with $\deg(h_j(x)) = l_j$ for $1 \le j \le t$.

By the CRT,

$$\begin{aligned}\frac{\mathbb{F}_q[x]}{(x^n-1)} &\simeq \frac{\mathbb{F}_q[x]}{(x-1)} \oplus \left(\bigoplus_{i=1}^{s}\frac{\mathbb{F}_q[x]}{(g_i(x))}\right) \oplus \left(\bigoplus_{j=1}^{t}\left(\left(\frac{\mathbb{F}_q[x]}{(h_j'(x))}\right)\oplus\left(\frac{\mathbb{F}_q[x]}{(h_j''(x))}\right)\right)\right)\\ &\simeq \mathbb{F}_q \oplus \left(\bigoplus_{i=1}^{s}\mathbb{F}_{q^{2k_i}}\right) \oplus \left(\left(\bigoplus_{j=1}^{t}\mathbb{F}_{q^{l_j}} \oplus \mathbb{F}_{q^{l_j}}\right)\right).\end{aligned}$$

In particular, each $\mathbb{F}_q[x]/(x^n-1)$-linear code C of length four can be decomposed as the 'CRT sum'

$$C \simeq C_0 \oplus \left(\bigoplus_{i=1}^{s} C_i\right) \oplus \left(\bigoplus_{j=1}^{t}(C_j' \oplus C_j'')\right),$$

where C_0 is a linear code over $\mathbb{F}_q$, C_i is a linear code over $\mathbb{F}_{q^{2k_i}}$ of length four for $1 \le i \le s$, and C_j' and C_j'' are linear codes over $\mathbb{F}_{q^{l_j}}$ of length four for $1 \le j \le t$. These codes are called the *constituents* of C.

Lemma 3.1 [5, Theorem 3.1]. *A four circulant code C over $\mathbb{F}_q[x]/(x^n-1)$ of length four is LCD with respect to the Hermitian inner product (or equivalently, a quasi-cyclic code of index four of length $4n$ over $\mathbb{F}_q$ is LCD with respect to the Euclidean inner product) if and only if the following conditions hold:*

(i) $C_0 \cap C_0^{\perp_E} = \{0\}$;
(ii) $C_i \cap C_i^{\perp_H} = \{0\}$, *for* $1 \le i \le s$;
(iii) $C_j'^{\perp_E} \cap C_j'' = \{0\}$ *and* $C_j' \cap C_j''^{\perp_E} = \{0\}$, *for* $1 \le j \le t$.

We now discuss the three conditions in Lemma 3.1 in more detail.

https://doi.org/10.1017/S0004972718000175 Published online by Cambridge University Press

Let ξ be a primitive nth root of unity over $\mathbb{F}_q$. Suppose that $g_i(\xi^{u_i}) = 0$ and $h_j(\xi^{v_j}) = 0$ for all i, j. Then $h_j^*(\xi^{(n-1)v_j}) = 0$. From the CRT, the respective generator matrices of C_0, C_i, C'_j and C''_j are G_0, G_i, G'_j and G''_j given by

$$G_0 = \begin{pmatrix} 1 & 0 & a(1) & b(1) \\ 0 & 1 & -b'(1) & a'(1) \end{pmatrix}, \quad G_i = \begin{pmatrix} 1 & 0 & a(\xi^{u_i}) & b(\xi^{u_i}) \\ 0 & 1 & -b'(\xi^{u_i}) & a'(\xi^{u_i}) \end{pmatrix},$$

$$G'_j = \begin{pmatrix} 1 & 0 & a(\xi^{v_j}) & b(\xi^{v_j}) \\ 0 & 1 & -b'(\xi^{v_j}) & a'(\xi^{v_j}) \end{pmatrix}, \quad G''_j = \begin{pmatrix} 1 & 0 & a(\xi^{(n-1)v_j}) & b(\xi^{(n-1)v_j}) \\ 0 & 1 & -b'(\xi^{(n-1)v_j}) & a'(\xi^{(n-1)v_j}) \end{pmatrix},$$

where $a(1), b(1), a'(1), b'(1) \in \mathbb{F}_q$, $a(\xi^{u_i}), b(\xi^{u_i}), a'(\xi^{u_i}), b'(\xi^{u_i}) \in \mathbb{F}_{q^{2k_i}}$, $a(\xi^{v_j}), b(\xi^{v_j})$, $a'(\xi^{v_j}), b'(\xi^{v_j}) \in \mathbb{F}_{q^{l_j}}$ and $a(\xi^{(n-1)v_j}), b(\xi^{(n-1)v_j}), a'(\xi^{(n-1)v_j}), b'(\xi^{(n-1)v_j}) \in \mathbb{F}_{q^{l_j}}$.

Condition (i) in Lemma 3.1. Since $a(1) = a'(1)$ and $b(1) = b'(1)$, then C_0 is an LCD code with respect to the Euclidean inner product if and only if

$$1 + a(1)c(1) + b(1)d(1) \neq 0. \tag{3.1}$$

Condition (ii) in Lemma 3.1. C_i is an LCD code with respect to the Hermitian inner product if and only if

$$-a(\xi^{u_i})b'^{q^{k_i}}(\xi^{u_i}) + b(\xi^{u_i})a'^{q^{k_i}}(\xi^{u_i}) \neq 0 \quad \text{or} \quad \begin{cases} -a(\xi^{u_i})b'^{q^{k_i}}(\xi^{u_i}) + b(\xi^{u_i})a'^{q^{k_i}}(\xi^{u_i}) = 0, \\ 1 + a(\xi^{u_i})a^{q^{k_i}}(\xi^{u_i}) + b(\xi^{u_i})b^{q^{k_i}}(\xi^{u_i}) \neq 0, \\ 1 + a'(\xi^{u_i})a'^{q^{k_i}}(\xi^{u_i}) + b'(\xi^{u_i})b'^{q^{k_i}}(\xi^{u_i}) \neq 0. \end{cases}$$

Using the Hermitian scalar product of [10, Remark 2], we see that the prime acts like conjugation $z \longmapsto z^q$ over $\mathbb{F}_{q^2}$ so that $a'(\xi^{u_i}) = a^{q^{k_i}}(\xi^{u_i})$. Thus C_i is an LCD code with respect to the Hermitian inner product if and only if

$$1 + a(\xi^{u_i})a^{q^{k_i}}(\xi^{u_i}) + b(\xi^{u_i})b^{q^{k_i}}(\xi^{u_i}) \neq 0. \tag{3.2}$$

Condition (iii) in Lemma 3.1. $C_j'^{\perp_E} \cap C''_j = \{0\}$ and $C'_j \cap C_j''^{\perp_E} = \{0\}$ for $1 \leq j \leq t$ if and only if

$$\begin{cases} 1 + b'(\xi^{v_j})b'(\xi^{(n-1)v_j}) + a'(\xi^{v_j})a'(\xi^{(n-1)v_j}) = \theta_1, \\ -a(\xi^{(n-1)v_j})b'(\xi^{v_j}) + b(\xi^{(n-1)v_j})a'(\xi^{v_j}) = \theta_2, \end{cases}$$

where θ_1 and θ_2 are not both zero, and

$$\begin{cases} 1 + a(\xi^{v_j})a(\xi^{(n-1)v_j}) + b(\xi^{v_j})b(\xi^{(n-1)v_j}) = \theta_3, \\ -a(\xi^{v_j})b'(\xi^{(n-1)v_j}) + b(\xi^{v_j})a'(\xi^{(n-1)v_j}) = \theta_4, \end{cases}$$

where θ_3 and θ_4 are not both zero. Since $a(\xi^{(n-1)v_j}) = a'(\xi^{v_j})$ and $b(\xi^{(n-1)v_j}) = b'(\xi^{v_j})$, the conditions are equivalent to

$$1 + a(\xi^{v_j})a'(\xi^{v_j}) + b(\xi^{v_j})b'(\xi^{v_j}) \neq 0.$$

https://doi.org/10.1017/S0004972718000175 Published online by Cambridge University Press

4. Exact enumeration

We assume that n is an odd integer, q is a prime power and $n|(q^\delta + 1)$ for some positive integer δ. Then $x^n - 1$ can be factored into a product of self-reciprocal irreducible polynomials.

We will enumerate the LCD four circulant codes over $\mathbb{F}_q$ when $n|(q^\delta + 1)$. From [9], if q is an odd prime, the so-called quadratic character η of $\mathbb{F}_q$ is given by $\eta(c) = (c/q)$ for $c \in \mathbb{F}_q^*$, the Legendre symbol from elementary number theory.

Lemma 4.1 [5, Appendix]. *If q is odd, then the number of solutions (x, y) in $\mathbb{F}_q$ of the equation $x^2 + y^2 = -1$ is $q - \eta(-1)$.*

Lemma 4.2 [5, Appendix]. *The number of solutions (x, y) in $\mathbb{F}_{q^2}$ of the equation $x^{1+q} + y^{1+q} = -1$ is $(q + 1)(q^2 - q)$.*

Now we can present the counting formula for four circulant self-dual codes over $\mathbb{F}_q$ when $n|(q^\delta + 1)$.

Theorem 4.3. *Suppose $n|(q^\delta + 1)$. Then $x^n - 1 = \alpha(x - 1) \prod_{i=1}^{s} g_i(x)$ over $\mathbb{F}_q$, where $\alpha \in \mathbb{F}_q^*$ and the $g_i(x)$ are self-reciprocal irreducible polynomials with degree $2k_i$ for $1 \le i \le s$. Furthermore, the total number of LCD four circulant codes over $\mathbb{F}_q$ is $\Omega_n = (q^2 - q + \eta(-1)) \prod_{i=1}^{s}(q^{3k_i} - q^{2k_i} + q^{k_i})$.*

Proof. From the preceding discussion and Lemma 3.1, we can count the number of LCD four circulant codes over $\mathbb{F}_q$ by counting their constituent codes. We first need to count the number of C_0. According to Lemma 4.1 and (3.1), there are $q^2 - q + \eta(-1)$ choices for $\{a(1), b(1)\}$. Next, we count the C_i by comparing Lemma 4.2 and (3.2). We find $q^{4k_i} - (q^{2k_i} + 1)(q^{2k_i} - q^{k_i}) = (q^{3k_i} - q^{2k_i} + q^{k_i})$ choices for $\{a(\xi^{u_i}), b(\xi^{u_i})\}$. Thus, the total number of codes over $\mathbb{F}_q$ is $(q^2 - q + \eta(-1)) \prod_{i=1}^{s}(q^{3k_i} - q^{2k_i} + q^{k_i})$. □

5. Relative distance bound

5.1. Special decomposition of $x^n - 1$. Let q be a primitive root modulo n where n is an odd prime. Recall that $x^n - 1 = (x - 1)(x^{n-1} + \cdots + x + 1) := (x - 1)M(x)$ where $M(x)$ is an irreducible polynomial over $\mathbb{F}_q$. The nonzero codewords of the cyclic code of length n generated by $M(x)$ are called *constant vectors*. The relative distance bound is based on the following auxiliary result.

Lemma 5.1. *Suppose the nonzero vector $z = (e(x), f(x), g(x), h(x)) \in (\mathbb{F}_q[x]/(x^n - 1))^4$ and $e(x)e'(x) + f(x)f'(x)$ is not a constant vector. Then there are at most $\lambda = q^2$ four circulant codes C over $\mathbb{F}_q[x]/(x^n - 1)$ such that $z \in C$.*

Proof. By the CRT,

$$\frac{\mathbb{F}_q[x]}{(x^n - 1)} \simeq \frac{\mathbb{F}_q[x]}{(x - 1)} \oplus \frac{\mathbb{F}_q[x]}{(M(x))} \simeq \mathbb{F}_q \oplus \mathbb{F}_{q^{n-1}}$$

https://doi.org/10.1017/S0004972718000175 Published online by Cambridge University Press

and

$$C \simeq C_0 \oplus C_1, \quad e(x) \simeq e_0 \oplus e_1, \quad f(x) \simeq f_0 \oplus f_1, \quad g(x) \simeq g_0 \oplus g_1, \quad h(x) \simeq h_0 \oplus h_1,$$

where $C_0 \subseteq \mathbb{F}_q^4$, $C_1 \subseteq \mathbb{F}_{q^{n-1}}^4$, $e_0, f_0, g_0, h_0 \in \mathbb{F}_q$ and $e_1, f_1, g_1, h_1 \in \mathbb{F}_{q^{n-1}}$.

Since ξ is the primitive root of unity over $\mathbb{F}_q$, there is an integer u_i such that ξ^{u_i} is a root of $M(x)$. The condition $z = (e(x), f(x), g(x), h(x)) \in C$ is equivalent to the two systems of equations

$$\begin{cases} g_0 = e_0a(1) - f_0b(1), & \text{that is } (e_0^2 + f_0^2)a(1) = e_0g_0 + f_0h_0, \\ h_0 = e_0b(1) + f_0a(1), & \text{that is } (e_0^2 + f_0^2)b(1) = e_0h_0 - f_0g_0, \end{cases}$$

and

$$\begin{cases} g_1 = e_1a(\xi^{u_i}) - f_1b'(\xi^{u_i}), & \text{that is } (e_1e_1^{q^{(n-1)/2}} + f_1f_1^{q^{(n-1)/2}})a(\xi^{u_i}) = e_1g_1^{q^{(n-1)/2}} + f_1h_1^{q^{(n-1)/2}}, \\ h_1 = e_1b(\xi^{u_i}) + f_1a'(\xi^{u_i}), & \text{that is } (e_1e_1^{q^{(n-1)/2}} + f_1f_1^{q^{(n-1)/2}})b(\xi^{u_i}) = h_1e_1^{q^{(n-1)/2}} - f_1g_1^{q^{(n-1)/2}}. \end{cases}$$

For the first constituent of C, there are two cases according to the value of $e_0^2 + f_0^2$.

(i) If $e_0^2 + f_0^2 \neq 0$, then there exists a unique solution for $\{a(1), b(1)\}$, where

$$a(1) = \frac{e_0g_0 + f_0h_0}{e_0^2 + f_0^2}, \quad b(1) = \frac{e_0h_0 - f_0g_0}{e_0^2 + f_0^2}.$$

(ii) If $e_0^2 + f_0^2 = 0$, then $a(\xi^{u_i})$ and $b(\xi^{u_i})$ are arbitrary elements in $\mathbb{F}_q$, and there are at most q^2 choices for $\{a(1), b(1)\}$.

For the second constituent of C, consider the unit character of $e_1e_1^{q^{(n-1)/2}} + f_1f_1^{q^{(n-1)/2}}$.

(i) If $e_1e_1^{q^{(n-1)/2}} + f_1f_1^{q^{(n-1)/2}} \neq 0$, then there exists a unique solution for $\{a(\xi^{u_i}), b(\xi^{u_i})\}$, where

$$a(\xi^{u_i}) = \frac{g_1e_1^{q^{(n-1)/2}} + f_1h_1^{q^{(n-1)/2}}}{e_1e_1^{q^{(n-1)/2}} + f_1f_1^{q^{(n-1)/2}}} \quad \text{and} \quad b(\xi^{u_i}) = \frac{h_1e_1^{q^{(n-1)/2}} - f_1g_1^{q^{(n-1)/2}}}{e_1e_1^{q^{(n-1)/2}} + f_1f_1^{q^{(n-1)/2}}}.$$

(ii) If $e_1e_1^{q^{(n-1)/2}} + f_1f_1^{q^{(n-1)/2}} = 0$, then $e(x)e'(x) + f(x)f'(x) = 0 \mod h(x)$ and $e(x)e'(x) + f(x)f'(x)$ is a constant vector, a contradiction.

Therefore, we obtain the desired result. □

5.2. Asymptotics of the relative distance. We derive the asymptotics for a family of codes for which we can apply an auxiliary result from number theory. Artin's conjecture (see [12]) states that for any integer $a \neq \pm 1$ or a perfect square, there are infinitely many primes p for which a is a primitive root (mod p). This conjecture was shown to be true by Hooley [6] based on the generalised Riemann hypothesis. With this assumption, there are infinite families of four circulant codes $C(4n)$ over $\mathbb{F}_q$ where the analysis made for $x^n - 1$ with only two irreducible factors applies.

https://doi.org/10.1017/S0004972718000175 Published online by Cambridge University Press

The q-ary Hilbert entropy function is defined for $0 \le t \le (q-1)/q$ by

$$H_q(t) = \begin{cases} 0 & \text{if } t = 0, \\ t\log_q(q-1) - t\log_q(t) - (1-t)\log_q(1-t) & \text{if } 0 < t \le (q-1)/q. \end{cases}$$

This quantity arises in the estimation of the volume of high-dimensional Hamming balls when the base field is $\mathbb{F}_q$. Namely, the volume of the Hamming ball of radius tn is asymptotically equivalent, up to subexponential terms, to $q^{nH_q(t)}$, when $0 < t < 1$ and n goes to infinity [7, Lemma 2.10.3]. This result can be used to establish an interesting relationship between Ω_n and λ.

Theorem 5.2. *Suppose n is an odd prime, $n > q$ and q is a primitive root modulo n. The family of LCD four circulant codes over $\mathbb{F}_q$ of length $4n$, of relative distance δ and rate $1/2$, satisfies $H_q(\delta) \ge \frac{3}{8}$. In particular, this family of codes is asymptotically good.*

Proof. Let Ω_n denote the size of the family. By Theorem 4.3,

$$\Omega_n = (q^2 - q + \eta(-1))(q^{3(n-1)/2} - q^{n-1} + q^{(n-1)/2}) \sim q^{3n/2}, \quad \text{as } n \to \infty,$$

for LCD four circulant codes. Assume we can prove that $\Omega_n > \lambda B(d_n)$ for n sufficiently large, where $B(r)$ denotes the number of vectors in $\mathbb{F}_q^{4n}$ with the Hamming weight of their $\mathbb{F}_q$ image less than r. From Lemma 5.1, the number of LCD four circulant codes satisfying the condition is less than $\lambda = q^2$.

Denote by δ the relative distance of this family of q-ary codes. Take d_n to be the largest number satisfying $\Omega_n > \lambda B(d_n)$ and assume a growth of the form $d_n \sim 4\delta_0 n$. Thus $\Omega_n \sim \lambda B(d_n)$ as $n \to \infty$. By the entropic estimate $B(d_n) \sim q^{4nH_q(\delta_0)}$ [7, Lemma 2.10.3], and our estimate for Ω_n, we obtain the estimate $H_q(\delta_0) = \frac{3}{8}$ for LCD four circulant codes. The result follows since $\delta \ge \delta_0$, from the definition of δ. □

References

[1] A. Alahmadi, C. Güneri, B. Özkaya, H. Shoaib and P. Solé, 'On self-dual double negacirculant codes', *Discrete Appl. Math.* **222** (2017), 205–212.

[2] A. Alahmadi, F. Ozdemir and P. Solé, 'On self-dual double circulant codes', *Des. Codes Cryptogr.* (to appear), doi:10.1007/s10623-017-0393-x.

[3] K. Betsumiya, S. Georgiou, T. A. Gulliver, M. Harada and C. Koukouvinos, 'On self-dual codes over some prime fields', *Discrete Math.* **262** (2003), 37–58.

[4] C. Carlet and S. Guilley, 'Complementary dual codes for counter-measures to side-channel attacks', *Amer. Inst. Math. Sci.* **10**(1) (2016), 131–150.

[5] C. Güneri, B. Özkaya and P. Solé, 'Quasi-cyclic complementary dual codes', *Finite Fields Appl.* **42** (2016), 67–80.

[6] C. Hooley, 'On Artin's conjecture', *J. reine angew. Math.* **225** (1967), 209–220.

[7] W. C. Huffman and V. Pless, *Fundamentals of Error Correcting Codes* (Cambridge University Press, New York, NY, 2003).

[8] A. Kaya, B. Yildiz and A. Pasa, 'New extremal binary self-dual codes from a modified four circulant construction', *Discrete Math.* **339** (2016), 1086–1094.

[9] R. Lidl and H. Niederreiter, *Finite Fields* (Addison-Wesley, Reading, MA, 1983).

[10] S. Ling and P. Solé, 'On the algebraic structure of quasi-cyclic codes I: finite fields', *IEEE Trans. Inform. Theory* **47**(7) (2001), 2751–2760.

[11] J. L. Massey, 'Linear codes with complementary duals', *Discrete Math.* **106–107** (1992), 337–342.
[12] P. Moree, 'Artin's primitive root conjecture - a survey', *Integers* **10**(6) (2012), 1305–1416.
[13] M. J. Shi, L. Q. Qian and P. Solé, 'On the self-dual negacirculant codes of index two and four', *Des. Codes Cryptogr.* (to appear), doi:10.1007/s10623-017-0455-0.
[14] M. J. Shi, H. W. Zhu and P. Solé, 'On the self-dual four-circulant codes', *Internat. J. Found. Comput. Sci.* (to appear), https://arxiv.org/pdf/1709.07548.pdf (2017).

HONGWEI ZHU, School of Mathematical Sciences, Anhui University,
Hefei, Anhui 230601, China
e-mail: zhwgood66@163.com

MINJIA SHI, Key Laboratory of Intelligent Computing and Signal Processing,
Ministry of Education, Anhui University, No. 3 Feixi Road, Hefei,
Anhui Province 230039, PR China
and
School of Mathematical Sciences of Anhui University, Anhui 230601, PR China
e-mail: smjwcl.good@163.com