AIMS Mathematics, 8(10): 23566–23577.
DOI: 10.3934/math.20231198
Received: 05 June 2023
Revised: 13 July 2023
Accepted: 24 July 2023
Published: 31 July 2023

http://www.aimspress.com/journal/Math

Research article

Double circulant codes for the Lee and Euclidean distance

Adel Alahmadi[1,*], **Altaf Alshuhail**[1,2], **Alaa Altassan**[3], **Hatoon Shoaib**[3] **and Patrick Solé**[4]

[1] Research Group of Algebraic Structures and Applications, Department of Mathematics, Faculty of Science, King Abdulaziz University, Jeddah, Saudi Arabia

[2] Mathematics Department, University of Hail, Hail, Saudi Arabia

[3] Mathematics Department, King Abdulaziz University, Jeddah, Saudi Arabia

[4] I2M (CNRS, Aix Marseille University, Centrale Marseille), Marseilles, France

* **Correspondence:** Email: analahmadi@kau.edu.sa.

Abstract: This paper investigates double circulant codes of length $2n$ over $\mathbb{Z}_{p^m}$ where p is an odd prime, n goes to infinity, and $m \geq 1$ is a fixed integer. Using random coding, we obtain families of asymptotically good Lee codes over $\mathbb{Z}_{p^m}$ in the case of small and large alphabets, and asymptotically good Euclidean codes over $\mathbb{Z}_{p^m}$ for small alphabets. We use Euclidean codes to construct spherical codes, and Lee codes to construct insertion/deletion codes, by a projection technique due to (Yaglom, 1958) for spherical codes, and to (Sok et al., 2018) for deletion codes.

Keywords: double circulant codes; Lee distance; Euclidean distance; spherical codes; deletion codes
Mathematics Subject Classification: 94B60, 94B75

1. Introduction

Double circulant codes over finite fields have been known to be asymptotically good for the Hamming distance for a long time [1, 5]. The proof relies on a polynomial representation of double circulant codes, along with some number theoretic conjecture (Artin primitive root conjecture [13]). In general, the Hamming distance is not a natural metric for measuring error correction capabilities of codes over rings [14], or more generally of codes over alphabets of size > 3, as attributing different weights to different nonzero symbols results into finer distances. For instance, the homogeneous metric is an important metric for ring alphabets. Thus, it was proved that double circulant codes over certain Galois rings are asymptotically good for the homogeneous distance [15].

In the present article, we shall consider double circulant codes over the rings $\mathbb{Z}_{p^m}$ where p is an odd prime, for the Lee and Euclidean distances, motivated by the following considerations.

The Lee metric is instrumental in constructing *insertions/deletion codes* [18] and the Euclidean metric is instrumental in constructing *spherical codes* [19]. In both cases, we use a projection technique due to Yaglom for spherical codes [11], and to [18] for insertion/deletion codes, that maps points within a ball in some dimension to the unit sphere in dimension one more. The Lee metric controls the Manhattan metric properties of lattices in constructed from codes over $\mathbb{Z}_{p^m}$. Similarly, the Euclidean metric over $\mathbb{Z}_{p^m}^N$ controls the standard Euclidean distance in the unit sphere of $\mathbb{R}^N$. For general background on, respectively, codes for the Lee metric, and codes for the Euclidean distance, we refer the reader respectively to [2, 3] and to [7].

We derive the relative Manhattan distance and the rate of asymptotic growth for balls in the Manhattan metric when the ambient space dimension goes to infinity and the radius is fixed. We also derive the relative square Euclidean distance and the rate of spherical asymptotic growth for balls in the Euclidean metric when the radius and size go to infinity.

By expurgated random coding techniques, we derive a lower bound on the relative Lee (resp. Euclidean) distance of double circulant codes over the said rings. The counting arguments involved in the proof rely on the polynomial representation of quasi-cyclic codes, and their analysis via the CRT for polynomials developed in [11, 12].

An outline of the paper is as follows. In Section 2, we provide some background material on Galois rings, Euclidean and Lee balls, and the algebraic structure of double circulant codes. Section 3 studies the asymptotic behavior of double circulant codes by the expurgated random coding argument made familiar by the Varshamov-Gilbert and Shannon bounds. Three cases are considered: Lee distance (small and large alphabets) and Euclidean distance. Section 4 concludes the article.

2. Preliminaries

2.1. Some rings

Throughout the paper, let p be an odd prime and m be a positive integer. The ring $\mathbb{Z}_{p^m}$ is the ring of integers modulo p^m. The Galois ring $GR(p^m, p^{mn})$ of order p^{mn}, and characteristic p^m is the Galois extension of $\mathbb{Z}_{p^m}$ with degree n. It is a local ring, with maximal ideal $\langle p\rangle$. The Teichmüller set $\mathcal{T} = \{x \in GR(p^m, p^{mn}) \mid x^{p^n} = x\}$ of $GR(p^m, p^{mn})$ is a set of representatives of the residue field $\mathbb{F}_{p^n} = GR(p^m, p^{mn})/\langle p\rangle$. It is known that $GR(p^m, p^{mn}) = \mathcal{T} \oplus p\mathcal{T} \oplus ... \oplus p^{m-1}\mathcal{T}$ so that any element $x \in GR(p^m, p^{mn})$ can be written as a base p decomposition of $GR(p^m, p^{mn})$, i.e., $x = \alpha_0 + p\alpha_1 + ... + p^{m-1}\alpha_{m-1}$ where $\alpha_i \in \mathcal{T}$ for $0 \leqslant i < m$. For motivation and background see [20].

2.2. Codes over $\mathbb{Z}_q$

A linear code C (for simply code) over $\mathbb{Z}_q$ of length N is a submodule of $\mathbb{Z}_q^N$. A code of length $2N$ is called double circulant over $\mathbb{Z}_q$ if its generator matrix G is of the form $G = (I, A)$, where I is the identity matrix of order N and A is a circulant matrix over $\mathbb{Z}_q$ of the same order.

The $\mathbb{Z}_q$-module $\mathbb{Z}_q^N$ is equipped with three natural distances [4] that we describe in the following three paragraphs.

2.2.1. Hamming distance

The Hamming distance between two codewords in C is the number of places where they differ, and it is denoted by d_H. The Hamming weight of any codeword in C is the number of nonzero components, and is denoted by w_H.

2.2.2. Lee distance

The Lee weight of an element $h \in \mathbb{Z}_q$ viewed as an integer $\in [0, q)$ is defined as follows:

$$w_L(h) \quad = \quad \min\{h, q-h\}.$$

The Lee weight of vectors $\mathbb{Z}_q^N$ (codewords in C) is the sum of Lee weight of its components. The Lee distance d_L between two integers $h_1, h_2 \in \mathbb{Z}_q$ is the Lee weight of $h_1 - h_2$. The Lee distance d_L between two vectors in $\mathbb{Z}_q^N$ (codewords in C), is the sum of the Lee distances between their corresponding components.

In [2], it is shown that the Lee weight of any nonzero vector $\mathbf{x} \in \mathbb{Z}_{p^m}^N$ is bounded from above and below as follows:

$$w_H(\mathbf{x}) \leq w_L(\mathbf{x}) \leq (\frac{p^m - 1}{2}) w_H(\mathbf{x}). \tag{2.1}$$

2.2.3. Euclidean distance

The Euclidean weight of any element h in $\mathbb{Z}_q$ can be defined directly as

$$w_E(h) \quad = \quad \min(h^2, (q-h)^2) = w_L(h)^2. \tag{2.2}$$

This notion can be extended to vectors in the obvious way, and the Euclidean distance between two vectors $\mathbf{x}$ and $\mathbf{y}$ on $\mathbb{Z}_q^N$ is then defined as $d_E(\mathbf{x}, \mathbf{y}) = w_E(\mathbf{x} - \mathbf{y})$. The minimum Euclidean distance d_E of a code C is then given by

$$d_E \quad = \quad \min\{d_E(c_i, c_j) \mid c_i, c_j \in C, \text{and } c_i \neq c_j\}.$$

As in [19], if $q = 2s + 1$, we will define the addressing map ϕ from $\mathbb{Z}_q$ into $\mathbb{R}$ by

$$\phi(h) = \begin{cases} h & \text{if } h \leq s, \\ -(q-h) & \text{if } h > s. \end{cases}$$

This map can be extended to vectors in the obvious way.

We remark that the Euclidean distance between two vectors $\mathbf{x}$ and $\mathbf{y}$ on $\mathbb{Z}_q^N$ satisfy the property

$$d_E(\mathbf{x}, \mathbf{y}) \quad = \quad (\phi(\mathbf{x}) - \phi(\mathbf{y}))^2.$$

2.3. Insertion/deletion codes in $\mathbb{Z}^N$

Following [18], we define the Manhattan distance between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^N$ as

$$d^1(\mathbf{x}, \mathbf{y}) \quad = \quad \sum_{i=1}^{N} |x_i - y_i|.$$

Define an $(N, d^1, \mathcal{N}, r)-$ code as a set of vectors of $\mathbb{Z}^n$, with pairwise Manhattan distance at least d^1, every coordinate at least r, and total sum of entries equal to $\mathcal{N}$. The addressing map Y_r to the ring $\mathbb{Z}_q$ uses the coset representatives $r, r+1, \ldots, r+q-1$ of $q\mathbb{Z}$ into $\mathbb{Z}$. We introduce a map $\Upsilon_{\mathcal{N}}$ from $\mathbb{Z}^N$ to $\mathbb{Z}^{N+1}$ defined by

$$\Upsilon_{\mathcal{N}}(\mathbf{x}) = (x_1, \ldots, x_N, \mathcal{N} - \sum_{i=1}^{N} x_i).$$

Note that $\mathcal{N} = \sum_{i=1}^{N} Y_r(x_i)$.

Proposition 1. *If C is a code over $\mathbb{Z}_q$ of length N and minimum Lee distance d_L over $\mathbb{Z}_q$, with the addressing Y_r, and $\mathcal{N} - N(q+r-1) > r$, then $\Upsilon_{\mathcal{N}} \circ Y_r(C)$ is an $(N+1, d^1, \mathcal{N}, r)-$ code in $\mathbb{Z}^{N+1}$ where its Manhattan distance is bounded below by the Lee distance of C.*

The coordinates of each codeword are at least r by Definition of Y_r. The last coordinate of the $\Upsilon_{\mathcal{N}}$ image is also $\geq r$ because $\sum_{i=1}^{N} x_i \leq N(q+r-1)$. The total sum of the entries of the $\Upsilon_{\mathcal{N}}$ image is $\mathcal{N}$ by Definition of $\Upsilon_{\mathcal{N}}$. The pairwise Manhattan distance of codewords is at least d^1, because the Manhattan distance is bounded below by the Lee distance. Note that the $\Upsilon_{\mathcal{N}}$ adds an extra entry to vectors which can only increase the Manhattan distance.

2.4. Spherical codes in $\mathbb{R}^N$

In this section we use [7], the ball of radius e in Euclidean N-space $\mathbb{R}^N$ is the set defined as

$$B(N, e) \quad = \quad \{(x_1, x_2, ..., x_N) \in \mathbb{R}^N | \sum_{i=1}^{N} x_i^2 \leqslant e^2\}.$$

The sphere of radius e in Euclidean N-space $\mathbb{R}^N$ is the set defined as

$$S(N, e) \quad = \quad \{(x_1, x_2, ..., x_N) \in \mathbb{R}^N | \sum_{i=1}^{N} x_i^2 = e^2\}.$$

When $e = 1$, $S(N, 1)$ is called the unit sphere. A spherical code $\mathcal{X}$ is a finite subset of $S(N, 1)$. The squared minimum distance ρ is the smallest squared distance between pairs of distinct codewords:

$$\rho(\mathbf{x}, \mathbf{y}) \quad = \quad min\{\sum_{i=1}^{N}(x_i - y_i)^2 \mid \mathbf{x} = (x_1, x_2, ..., x_N), \mathbf{y} = (y_1, y_2, ..., y_N) \in \mathcal{X}, \mathbf{x} \neq \mathbf{y}\}.$$

Following [19], we embed $\mathbb{R}^N$ into $\mathbb{R}^{N+1}$ by the Yaglom map

$$\mathrm{Y} \quad : \quad (x_1, ..., x_N) \mapsto (x_1, ..., x_N, \sqrt{e^2 - \sum_{i=1}^{N} {x_i}^2}).$$

Note that this map sends the ball $B(N+1, e)$ of radius e in $\mathbb{R}^N$ into the sphere $S(N+1, e)$ with radius e in $\mathbb{R}^{N+1}$.

Proposition 2. *[19] Let $q = 2s + 1$. If C is a code of length N and minimum Euclidean distance d_E over $\mathbb{Z}_q$, then $\mathrm{Y}(\phi(C))$ is a spherical code lying in the sphere $S(N, s\sqrt{N})$ of squared Euclidean distance d_E.*

2.5. Algebraic structure of double circulant codes of odd length

From now on, we assume that n is an odd integer, and $gcd(n, p^m) = 1$. We can cast the factorization of $x^n - 1$ into distinct basic irreducible polynomials over $\mathbb{Z}_{p^m}$ in the form

$$x^n - 1 \quad = \quad \mu(x-1)\prod_{i=2}^{u} g_i(x)\prod_{i=1}^{t} h_i(x)h_i^*(x), \tag{2.3}$$

where μ nonzero unit in $\mathbb{Z}_{p^m}$, $g_i(x)$ is a self-reciprocal polynomial with degree $2e_i$ for $2 \le i \le u$, and $h_j^*(x)$ is the reciprocal polynomial of $h_j(x)$ with degree b_j for $1 \le j \le t$. By the Chinese Remainder Theorem (CRT), we have

$$\begin{aligned}\frac{\mathbb{Z}_{p^m}[x]}{\langle x^n-1\rangle} &\simeq \frac{\mathbb{Z}_{p^m}[x]}{\langle x-1\rangle} \oplus \Big(\bigoplus_{i=2}^{u} \frac{\mathbb{Z}_{p^m}[x]}{\langle g_i(x)\rangle}\Big) \oplus \bigoplus_{j=1}^{t}\Big(\frac{\mathbb{Z}_{p^m}[x]}{\langle h_j(x)\rangle} \oplus \frac{\mathbb{Z}_{p^m}[x]}{\langle h_j^*(x)\rangle}\Big)\\ &\simeq \mathbb{Z}_{p^m} \oplus \Big(\bigoplus_{i=2}^{u} GR(p^m, p^{2me_i})\Big) \oplus \Big(\bigoplus_{j=1}^{t} GR(p^m, p^{mb_j}) \oplus GR(p^m, p^{mb_j})\Big).\end{aligned}$$

Note that all of these rings are extensions of $\mathbb{Z}_{p^m}$. Let $\mathcal{R}_n = \frac{\mathbb{Z}_{p^m}[x]}{\langle x^n-1\rangle}$. This decomposition naturally extends to $\mathcal{R}_n^2$ as follows

$$\mathcal{R}_n^2 \quad \backsimeq \quad \mathbb{Z}_{p^m}^2 \oplus \Big(\bigoplus_{i=2}^{u} GR(p^m, p^{2me_i})^2\Big) \oplus \Big(\bigoplus_{j=1}^{t}(GR(p^m, p^{mb_j}))^2 \oplus GR((p^m, p^{mb_j}))^2\Big).$$

In particular, each linear code C of length 2 over $\mathbb{Z}_{p^m}$ can be decomposed as the -CRT sum-

$$C \quad = \quad C_1 \oplus \bigoplus_{i=2}^{u} C_i \oplus \bigoplus_{j=1}^{t}(C_j' \oplus C_j'').$$

So C can be viewed as a submodule of $\mathcal{R}_n^2$, with generator $\langle 1, a(x)\rangle$, where the x- expansion of $a(x) \in \mathbb{Z}_{p^m}[x]$ is the first row of A.

2.6. Codes over $\mathbb{Z}_p$ and asymptotic bounds

Let C be a code of length N over $\mathbb{Z}_p$. This code is linear if it is a $\mathbb{Z}_p$-vector subspace of $\mathbb{Z}_p^N$. The dimension of a code C, denoted by k, is equal to its dimension as a vector space.

The three parameters of a code are written compactly as $[N, k, d_H]$, $[N, k, d_L]$ or $[N, k, d_E]$, depending on the distance considered. When we extend this notation to code C that is a submodule of $\mathbb{Z}_q^N$, then $k = \log_q(|C|)$ where $|C|$ is the number of codewords in C. Let $C(N)$ be a family of codes with parameters $[N, k_N]$. The rate of $C(N)$ is defined to be $R = \limsup_{N\to\infty} \frac{k_N}{N}$. The relative minimum distance δ depends on the third parameters as follows:

Remark 3. *Let $s = \frac{q-1}{2}$. If $C(N)$ a family of codes with the following distances:*

(i) Hamming distance $d_{H,N}$, then its relative Hamming distance is $\delta_H = \liminf_{N\to\infty} \frac{d_{H,N}}{N}$.

(ii) Lee distance $d_{L,N}$, then is its relative Lee distance is $\delta_L = \liminf_{N\to\infty} \frac{d_{L,N}}{sN}$.

(iii) Euclidean distance $d_{E,N}$, then its relative Euclidean distance is $\delta_E = \liminf_{N\to\infty} \frac{d_{E,N}}{s^2N}$.

A family of codes is said to be good if $R\delta \neq 0$.

Let $V_L(N, e, q)$ (resp. $V_E(N, e, q)$) denote the size of the Lee (resp. Euclidean) sphere of radius e, and let us define $A_L(N, d_L, q)$ (resp. $A_E(N, d_E, q)$) to be the maximal number of codewords in a code of length N over $\mathbb{Z}_q$ with Lee (resp. Euclidean) distance d_L (resp. d_E).

The following Theorem is the analogue of the standard Gilbert bound of the Hamming metric in the Lee and Euclidean metric. The standard proof is omitted.

Theorem 4. *There are codes in $\mathbb{Z}_q^N$ of Lee distance d_L and of cardinality*

$$A_L(N, d_L, q) \geq \frac{q^N}{V_L(N, d_L - 1, q)}.$$

There are codes in $\mathbb{Z}_q^N$ of Euclidean distance d_E and of cardinality

$$A_E(N, d_E, q) \geq \frac{q^N}{V_E(N, d_E - 1, q)}.$$

The following three theorems give the asymptotic exponent of $V_L(N, e, q)$ (resp. $V_E(N, e, q)$) for N large and $e = s\tau N$, where $0 \leq \tau \leq 1$, and with the standard definition of the rate and relative minimum distance of the family of codes $C(N)$. Their respective corollaries are the analogues of the classical Asymptotic Gilbert-Varshamov Bound [9] for, respectively, the Lee distance (first small alphabets, then large alphabets) or the Euclidean distance. For simplicity'sake we concentrate on the case of p odd.

2.6.1. Lee balls for small alphabets

If we denote

$$l(\tau, q) = \lim_{N\to\infty}(1 - \frac{1}{N}\log_q(V_L(N, s\tau N, q))),$$

where $0 \leq \tau \leq 1$.

Theorem 5. *[3] If $q = 2s + 1$, then $l(\tau, q) = 1 + \log_q \alpha\beta^{s\tau}$, where $\alpha \geqslant 0, \beta \geqslant 0$ satisfy*

$$\alpha + 2\alpha\sum_{i=1}^{s}\beta^i = 1,$$
$$\alpha\sum_{i=1}^{s} i\beta^i = \frac{\tau.s}{2},$$

where $0 \leqslant \tau \leqslant (q + 1)/2q$. Moreover, $l(\tau, q) = 0$ if $(q + 1)/2q \leqslant \tau \leqslant 1$.

Corollary 6. *[3] If $0 < \delta_L \leq \frac{q+1}{2q}$ where $q \geq 2$, then*

$$R \geq l(\delta_L, q)$$

where $R = \liminf_{n\mapsto\infty} \frac{1}{n}\log_q A_L(n, s\delta_L n, q)$.

2.6.2. Lee balls for large alphabets

Theorem 7. *[19] For $q \geqslant 2r+1$, for large N and $\frac{r}{N}$ tending to ω, we obtain*

$$\lim_{N\to\infty} \frac{1}{N} \log_q(V_L(N,e,q)) \quad = \quad L_q(\omega) + o(1),$$

where

$$L_q(x) = x\log_q(x) + \log_q(x + \sqrt{x^2+1}) - x\log_q(\sqrt{x^2+1} - 1).$$

Corollary 8. *[19] If $0 < \delta_L \leq L_q(1)$ where $q \geq 2\delta_L N + 1$, then*

$$R \quad \geq \quad 1 - L_q(\delta_L).$$

2.6.3. Euclidean balls for small alphabets

Theorem 9. *[8] The asymptotic exponent of $V_E(N,e,q)$ for N large and $e = \lfloor \tau N \rfloor$ is*

$$\lim_{N\to\infty} \frac{1}{N} \log_q(V_E(N,r,q)) = E(\tau,q),$$

where $E(\tau,q) = \log_q(f(\mu)) - \tau\log_q(\mu)$ and μ is the unique real positive solution of $zf'(z) = \tau f(z)$, and $f(z) = 1 + 2\sum_{i=1}^{s} z^{i^2}$.

Corollary 10. *[8] If $0 < \delta_E \leq 1 - \frac{1}{q}$ where $q = 2s+1$, then*

$$R \quad \geq \quad 1 - E(s^2\delta_E, q).$$

3. Main results

This section is only for the special case of the factorization of $x^n - 1$ over $\mathbb{Z}_{p^m}$ into exactly two basic irreducible polynomials. In particular, for $m = 1$, the existence of such a factorization for infinitely many n's will depend on Artin primitive root conjecture, which is known to hold under Generalized Riemann Hypothesis (GRH), and is proved by Hath-Brown for all but a finite number of primes [13]. Lifting such a factorization, for fixed n, from $\mathbb{F}_p$ to $\mathbb{Z}_{p^m}$ is ensured by Hensel lifting [20]. Let C_a denotes the double circulant code generated by $\langle 1, a\rangle$, where $a = a(x)$ is a polynomial in $\mathbb{Z}_{p^m}[x]$.

3.1. Long Lee double circulant codes

Theorem 11. *From the above assumptions. If $f, g \in \mathbb{Z}_{p^m}^n$ such that $(0,0) \neq (f,g)$, and (f,g) has Lee weight less than n, then the vector (f,g) gives at most λ double circulant codes over $\mathbb{Z}_{p^m}$ of length $2n$ with $\lambda = p^{(m-1)n+1}$.*

By the CRT, $(f,g) \simeq (f_1,g_1) \oplus (f_2,g_2)$ where f_1 and $g_1 = a_1 f_1$ as elements of $\mathbb{Z}_{p^m}$, f_2 and $g_2 = a_2 f_2$ as elements of $GR(p^m, p^{m(n-1)})$. Consider $C_{a_1} = \langle [1,a_1]\rangle$, and $C_{a_2} = \langle [1,a_2]\rangle$. Let $(f_1,g_1) \in C_{a_1}$ and $(f_2,g_2) \in C_{a_2}$. Determining a is equivalent to determining the pair (a_1,a_2).

We distinguish the following cases:

i. If f_1 is a unit, then a_1 is uniquely determined by $g_1 = a_1 f_1$.

ii. If $(f_1 \neq 0)$ is not a unit, where $f_1 = p^h f_1'$ such that f_1' is a unit and $1 \leq h \leq m-1$, we then obtain $g_1 = p^h g^*$ where $g^* \in \mathbb{Z}_{p^m}$, which implies $a_1 f_1' - g^* = p^{m-h}\alpha$ where $\alpha = \sum_{i=0}^{h-1} \alpha_i p^i$. Each α_i for $0 \leq i \leq h-1$ can take at most p values. So a_1 takes at most $p^h \leq p^{(m-1)}$ values.

iii. If $f_1 = 0$, then a_1 can take at most p^m values.

iii-1. If $f_2 = 0$, then $(f, g) = (0, 0)$, a contradiction as (f, g) is a nonzero vectors.

iii-2. If f_2 is a unit then a_2 is uniquely determined by the equation $g_2 = a_2 f_2$. So a has p^m values.

iii-3. If $f_2 \neq 0$ is not a unit, the case is similar to that of f_1 with α having at most $p^{h(n-1)}$ values by the p-adic representation in $GR(p^m, p^{m(n-1)})$. Thus a_2 has at most $p^{(n-1)(m-1)}$ since $h \leq m-1$. It follows that a has $p^m p^{(m-1)(n-1)}$ values.

iv. If $f_1 \neq 0$ and $f_2 \neq 0$ are not units, then by (ii) and (iii-3) a has at most $p^{n(m-1)}$ values.

v. If $f_1 \neq 0$ and $f_2 \neq 0$ are units, then $a = \frac{g}{f}$ has a unique solution.

vi. If $f_1 \neq 0$ is not a unit and $f_2 = 0$, we then obtain $w_H(f) = n$, and by (1.4.1) we have $w_L((f, g)) > n$, a contradiction with the hypothesis.

Thus, we obtain that there are at most $\lambda = p^m p^{(m-1)(n-1)} = p^{n(m-1)+1}$ double circulant codes over $\mathbb{Z}_{p^m}$ of length $2n$.

The following results use that fact that the volumes of Lee balls for (large and small alphabets) with radius $s\delta_0 N$ are, up to subexponential terms, $p^{Nm(L_{p^m}(s.\delta_0)+o(1))}$ (resp. $p^{Nm(1-l(\delta_0,p^m))}$), when $0 < \delta_0 < 1$ and N go to infinity.

Theorem 12. *Let $p = 2s+1$ and $p^m \geqslant 2a+1$ with $a = 2sn\delta_0$ such that $\delta_0 \in (0,1)$. Then the family of double circulant codes over $\mathbb{Z}_{p^m}$ with length $2n$, rate $\frac{1}{2}$, and relative distance δ_L, satisfies $\delta_L \geq L_{p^m}^{-1}(\frac{1}{2m})s^{-1}$. In particular, that family of codes is good.*

Let $p^m = 2s+1$ be fixed, and let Ω_n denote the size of the family of double circulant codes over $\mathbb{Z}_{p^m}$ of length $2n$. Thus, for $n \to \infty$ we have $\Omega_n \sim p^{mn}$. Assume we can prove that for n large enough $\Omega_n > \lambda_n V(2n, d_{L,n}, p^m)$. Here $\lambda_n = p^{n(m-1)+1}$. This would imply, by Theorem 11, that there are double circulant codes of length $2n$ in the family with minimum Lee distance greater than or equal $d_{L,n}$. Let δ_L be the relative Lee distance of this family. If we take $d_{L,n}$ to be the largest number satisfying $\Omega_n > \lambda_n V(2n, d_{L,n}, p^m)$, and assume a growth of the form $d_{L,n} \sim 2sn\delta_o$, then $\Omega_n \sim \lambda_n V(2n, d_{L,n}, p^m)$ for $n \to \infty$ using the large alphabets entropic estimate for $V_L(2n, d_{L,n}, p^m) \sim p^{2nm(L_p(s\delta_o)+o(1))}$, with values of Ω_n and λ_n, with the estimate $\delta_o = L_{p^m}^{-1}(\frac{1}{2m})s^{-1}$. The result follows by observing that, by definition of δ_L, $\delta_L \geq \delta_o$.

The next Theorem follows by using a similar argument as in the proof of Theorem 12.

Theorem 13. *Let $p^m = 2s+1$. Then the family of double circulant codes over $\mathbb{Z}_{p^m}$ of length $2n$, and rate $\frac{1}{2}$, of relative distance δ_L,satisfies $\delta_L \geq l^{-1}(\frac{2m-1}{2m}, p^m)$. In particular, that family of codes is good.*

By [8], assume that d^1, r are fixed, $\mathcal{N} \to \infty$, and $n \sim \eta\mathcal{N}/r$, for some constant $\eta \in (0,1)$. Denote by R^1 the asymptotic rate of a family of $(2n, d^1, \mathcal{N}, r)$-codes C_n, and the rate is given as follows

$$R^1 = \limsup_{\mathcal{N}\to\infty} \frac{1}{\mathcal{N}} \log_2 |C_n|.$$

Corollary 14. *There is a family of* $(2n+1, d^1, N, r)$*-codes over* $\mathbb{Z}$ *of relative Manhattan distance at least* $l^{-1}(\frac{2m-1}{2m}, p^m)$*, and rate* R^1*, which satisfies* $R^1 = \frac{\eta m}{r}\log_2 p$*.*

Let d^1, r be fixed, by Theorem 13, there is a family of double circulant codes C denoted by Ω_n over $\mathbb{Z}_{p^m}$ of length $2n$ and of Lee distance at least d_L and by Proposition 1, there is a family of $(2n+1, d^1, \mathcal{N}, r)$- codes up to normalization $\Upsilon_{\mathcal{N}}(Y_r(C))$ of $\mathbb{Z}^{2n+1}$, and its rate satisfies $R^1 = \frac{1}{\mathcal{N}}\log_2 p^{mn} \Rightarrow R^1 = \frac{\eta m}{r}\log_2 p$.

In Table 1, values of δ_L are listed for some values of p^m. If $C(n)$ is a family of codes of parameters $[n, k_n, d_{L,n}]$, then by Corollary 14 $l(\delta_L, p^m) = \frac{2m-1}{2m}$.

Table 1. Values of δ_L are listed for some values of p^m.

m	p	p^m	δ_L
1		3	0.159
2	3	9	0.0385
3		27	0.011
1		5	0.134
2	5	25	0.022
3		125	0.00429
1		7	0.118
2	7	49	0.0148
3		343	0.002

3.2. Long Euclidean double circulant codes

Theorem 15. *If* $f, g \in \mathbb{Z}^n_{p^m}$ *such that* $(f, g) \neq (0, 0)$ *, and* (f, g) *has Euclidean weight less than n, then there are at most* $p^{(m-1)n+1}$ *polynomials a such that* $(f, g) \in C_a$*.*

We can prove this result in the same manner as Theorem 11. By using Eqs (2.1) and (2.2), we get $w_H \leqslant w_L \leqslant w_E$. It follows that there are at most $p^{(m-1)n+1}$ polynomials a such that $(f, g) \in C_a$.

Theorem 16. *Let* $p^m = 2s+1$*. Then the family of double circulant codes over* $\mathbb{Z}_{p^m}$ *of length* $2n$*, rate* $\frac{1}{2}$*, and relative distance* δ_E*, satisfies* $\delta_E \geq E^{-1}(\frac{1}{2m}, p)\cdot s^{-2}$*. In particular, these families of codes are good.*

By applying Theorem 9 in the case where the radius of the Euclidean sphere is $2s\delta_E n$, and using a similar technique to the proof of Theorem 12 the result follows.

In Table 2, values of δ_E are listed for some values of p^m. If $C(n)$ is a family of Euclidean codes of parameters $[n, k_n, d_{E,n}]$, then by Theorem 16 $E(s^2\cdot\delta_E, p^m) = \frac{1}{2m}$.

Following [6], let R denotes the asymptotic binary rate of a family of spherical codes $\mathcal{X}$, and the rate is given as follows

$$R = \lim_{N\to\infty}\frac{\log_2(|\mathcal{X}|)}{N}. \tag{3.1}$$

In [10] a lower bound of Shannon is given a lower bound on the binary rate of a spherical code R_S of a given $0 \leq \tau \leq 1$

$$R \leq R_S(\tau) = 1 - \frac{1}{2}\log_2(\tau(4-\tau)). \tag{3.2}$$

Table 2. Values of δ_E are listed for some values of p^m.

m	p	p^m	δ_E
1		3	0.159
2	3	9	0.996×10^{-2}
3		27	0.943×10^{-3}
1		5	0.723
2	5	25	0.996×10^{-2}
3		125	0.753×10^{-4}
1		7	0.454×10^{-2}
2	7	49	0.710×10^{-3}
3		343	0.139×10^{-4}

From Theorem 16 and Proposition 2, the following corollary immediately follows.

Corollary 17. *Let $p^m = 2s + 1$. There is a family of spherical codes up to normalization $Y(\phi(C))$ of $\mathbb{R}^{2n+1}$, binary rate $\frac{m\log_2 p}{2}$, and relative squared distance $\delta_E \geq E^{-1}(\frac{1}{2m}, p)s^{-2}$.*

In Table 3 is shown that comparison between $R(\delta_E)$ and $R_S(\delta_E)$ where δ_E is given in previous corollary.

Table 3. Comparison between $R(\delta_E)$ and $R_S(\delta_E)$.

m	p	p^m	δ_E	R	$R_S(\delta_E)$
1		3	0.159	0.792	1.353
2	3	9	0.996×10^{-2}	1.584	3.326
3		27	0.943×10^{-3}	2.377	5.0252
1		5	0.723	1.160	1.907
2	5	25	0.996×10^{-2}	2.321	3.326
3		125	0.753×10^{-4}	3.482	6.848
1		7	0.454×10^{-2}	1.403	2.237
2	7	49	0.710×10^{-3}	2.807	5.229
3		343	0.139×10^{-4}	4.211	8.0621

4. Conclusions

In this paper we have proved the existence of asymptotically good families of double circulant codes for the Lee distance and the Euclidean distance. The motivation was to construct spherical codes from Euclidean distance codes and insertions/deletion codes in the case of the Lee distance. There are certainly some more applications in the domain of Euclidean lattices, or lattices for the Manhattan metric obtained from codes by the so-called Construction A [11]. At a more technical level, considering quasi-cyclic codes of index higher than 2, extending these results to three- and four-circulant codes and to their negacirculant counterparts following the paths in [16, 17] is a worthwhile project.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia under grant no. (KEP-Msc-28-130-40). The authrs, therefore, acknowledge with thanks DSR techical and financial support.

Conflict of interest

Prof. Patrick Solé is the Guest Editor of special issue "Mathematical Coding Theory and its Applications" for AIMS Mathematics. Prof. Patrick Solé was not involved in the editorial review and the decision to publish this article.

All authors declare no conflicts of interest in this paper.

References

1. A. Alahmadi, F. Özdemir, P. Solé, On self-dual double circulant codes, *Des. Codes Cryptogr.*, **86** (2018), 1257–1265. https://doi.org/10.1007/s10623-017-0393-x
2. J. Astola, *The theory of Lee-codes*, Lappeenranta University of Technology, 1982.
3. J. Astola, On the asymptotic behaviour of Lee-codes, *Discrete Appl. Math.*, **8** (1984), 13–23. https://doi.org/10.1016/0166-218X(84)90074-X
4. G. Bini, F. Flamini, *Finite commutative rings and their applications*, Springer, 2002. https://doi.org/10.1007/978-1-4615-0957-8
5. C. L. Chen, W. W. Peterson, E. J. Weldon, Some results on quasi-cyclic codes, *Inf. Control*, **15** (1969), 407–423. https://doi.org/10.1016/S0019-9958(69)90497-5
6. J. H. Conway, N. J. A. Sloane, *Sphere packings, lattices and groups*, Springer, 1993.
7. T. Ericson, V. Zinoviev, *Codes on Euclidean spheres*, North-Holland, 2001.
8. D. Gardy, P. Solé, Saddle point techniques in asymptotic coding theory, In: G. Cohen, A. Lobstein, G. Zémor, S. Litsyn, *Algebraic coding*, Lecture Notes in Computer Science, Springer, **573** (1992), 75–81. https://doi.org/10.1007/BFb0034343
9. W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511807077
10. G. Lachaud, J. Stern, Polynomial-time construction of codes. II. spherical codes and the kissing number of spheres, *IEEE Trans. Inf. Theory*, **40** (1994), 1140–1146. https://doi.org/10.1109/18.335961
11. S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes. I. Finite fields, *IEEE Trans. Inf. Theory*, **47** (2001), 2751–2760. https://doi.org/10.1109/18.959257

12. S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes II: chain rings, *Des. Codes Cryptogr.*, **30** (2003), 113–130. https://doi.org/10.1023/A:1024715527805
13. P. Moree, Artin's primitive root conjecture–a survey, *Integers*, **12** (2012), 1305–1416. https://doi.org/10.1515/integers-2012-0043
14. M. Shi, A. Alahmadi, P. Solé, *Codes and rings: theory and practice*, Academic Press, 2017. https://doi.org/10.1016/C2016-0-04429-7
15. M. Shi, D. Huang, L. Sok, P. Solé, Double circulant self-dual and LCD codes over Galois rings, *Adv. Math. Commun.*, **13** (2019), 171–183. https://doi.org/10.3934/amc.2019011
16. M. Shi, L. Qian, P. Solé, On self-dual negacirculant codes of index two and four, *Des. Codes Cryptogr.*, **86** (2018), 2485–2494. https://doi.org/10.1007/s10623-017-0455-0
17. M. Shi, H. Zhu, L. Qian, P. Solé, On self-dual four circulant codes, *Int. J. Found. Comput. Sci.*, **29** (2018), 1143–1150. https://doi.org/10.1142/S0129054118500259
18. L. Sok, J. C. Belfiore, P. Solé, A. Tchamkerten, Lattice codes for the deletion and repetition channels, *IEEE Trans. Inf. Theory*, **64** (2018), 1595–1603. https://doi.org/10.1109/TIT.2018.2791990
19. P. Solé, J. C. Belfiore, Constructive spherical codes near the Shannon bound, *Des. Codes Cryptogr.*, **66** (2013), 17–26. https://doi.org/10.1007/s10623-012-9633-2
20. Z. X. Wan, *Lectures on finite fields and Galois rings*, World Scientific, 1997. https://doi.org/10.1142/5350

AIMS Press